Adjusting Sensing Range to Maximize Throughput on Ad-Hoc Multi-Hop Wireless Networks

THESIS

Christopher K. Roberts, Second Lieutenant, USAF

AFIT/GCS/ENG/03-17

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCS/ENG/03-17

Adjusting Sensing Range to Maximize Throughput on Ad-Hoc Multi-Hop Wireless Networks

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Christopher K. Roberts, B.S.

Second Lieutenant, USAF

March, 2003

AFIT/GCS/ENG/03-17

Adjusting Sensing Range to Maximize Throughput on Ad-Hoc Multi-hop Wireless Networks

Christopher K. Roberts, B.S.

Second Lieutenant, USAF

Approved:

Major Rusty Baldwin, PhD Thesis Advisor	13 Mar 03 Date
Dr Richard Raines Committee Member	13 Mar 03 Date
Dr Michael Temple Committee Member	13 Mar 03 Date

Contents

List of Figures

Figure		Page

List of Tables

List of Abbreviations

Abbreviation	
(ANOVA)	ANalysis Of VAriance
(BPSK)	Binary Phase Shift Keying
(BTMA)	Busy Tone Multiple Access
(CCA)	Clear Channel Assessment
(CSMA)	Carrier Sense Multiple Access
(CSMA/CA)	Carrier Sense Multiple Access with Collision Avoidance
(CSMA/CD)	Carrier Sense Multiple Access with Collision Detection
(CDMA)	Code Division Multiple Access
(CTS)	Clear To Send
(CUT)	Component Under Test
(DBTMA)	Dual Busy Tone Multiple Access
(DCF)	Distributed Coordination Function
(DIFS)	DCF Inter-Frame Spacing
(DSSS)	Direct Sequenced Code Division Multiple Access
(EY-NPMA)	Elimination Yield Non-pre-emptive Priority Multiple Access
(FDMA)	Frequency Division Multiple Access
(FHSS)	Frequency Hopping Spread Spectrum
(MAC)	Medium Access Control
(MACA)	Multiple Access with Collision Avoidance
(Mbps)	Megabits per second
(NAK)	Negative Transmission Acknowledgement
(OSI)	Open Systems Interconnection
(PCF)	Point Coordination Function
(RTDMA)	Random-TDMA
(RTS)	Request to Send
(TDMA)	Time Division Multiple Access

Abbreviation

(SIFS)	Short Inter-frame Space
(SUT)	System Under Test
(WCD)	Wireless Collision Detect

AFIT/GCS/ENG/03-17

Abstract

The use of ad-hoc wireless networks is becoming increasingly common within the United States Air Force. Such networks are able to be implemented where traditional wired networks are either impractical or too expensive. As the miniaturization of communication devices continues, it is becoming increasingly common for mobile devices to communicate directly with each other, eliminating the need for central access points. Such a network is referred to as a multi-hop ad-hoc network, or simply a multi-hop network.

Most multi-hop network protocols use some form of carrier sensing to determine if the wireless channel is in use. A large sensing range can reduce packet collisions. However, it can also decrease spatial reuse. Conversely, a smaller sensing range can lead to higher spatial reuse but increase packet collisions.

This study examines a variety of multi-hop network topologies, sizes and traffic loads and determines the sensing range for each that maximizes network throughput. In most instances, a sensing range twice as large as the node's communication range yields maximum or near maximum network throughput. However, results indicate a shorter sensing range can be better if it provides a significant increase in spatial reuse.

Adjusting Sensing Range to Maximize Throughput on Ad-Hoc Multi-Hop Wireless Networks

I. *Introduction*

This chapter introduces the research effort. After providing a brief background on the subject area, it defines the problem under study and its significance. Finally, this chapter defines research goals and the document organization.

1.1 Background

With the continued miniaturization of communication devices, and the military's increased dependence upon them, ad-hoc networks are becoming increasingly common within military environments. Ad-hoc networks are wireless networks that do not rely on static access points. In an ad-hoc network, wireless nodes communicate directly with each other. For example, an ad-hoc network allows communication between several nodes in a remote location. The simplest ad-hoc networks are fully-connected, meaning all nodes can directly communicate with every other node. As ad-hoc networks become larger, it may not be possible for a node at one network extreme to communicate with a node at the other. For such nodes to communicate, one or more intermediate nodes must relay the messages. A network having relay capability is called a multi-hop ad-hoc network, or simply a multi-hop network. Every node in a multi-hop network can potentially serve as a router.

The IEEE 802.11 standard is commonly used in wireless networking. The protocol uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme to allow multiple nodes to share the wireless channel. Using this scheme, a node desiring to transmit first senses the channel to determine if the energy level is above a certain threshold. If the threshold is exceeded, the station determines

the channel is busy and defers, meaning it waits a certain amount of time before re-sensing the channel. This process is known as Clear Channel Assessment (CCA). The sensing threshold value determines the sensing range (R_S) for the node. Conversely, the node transmit power determines the node communication range (R_C).

CSMA works well in a fully connected network where propagation delays are low. When this is not true, the possibility of hidden and exposed nodes arises. Nodes are considered *hidden* from each other if they can communicate to a third node but are undetectable to each other. An *exposed* node is one whose transmission causes another node to defer transmission, even when no collision would have resulted if it had transmitted. Both hidden and exposed nodes reduce network throughput.

In a fully connected network, the ideal sensing range is one that minimizes collisions as Figure 1.1 illustrates. Node A must not transmit when another node within A's interference range (R_{I_A}) is receiving data, e.g., node B. In a worst case, node B is located on the interference range border as illustrated. Node C represents the furthest node from B that can communicate to B. Thus, B is within the communication range of C (R_{C_C}). From this representation, it can be seen that to minimize collisions between packets from A and C that simultaneously arrive at B, A must have a sensing range $R_{S_A} \geq R_{I_A} + R_{C_C}$ such that A can detect (sense) that C is transmitting. Since a node's interference range is at least equal to the communication range, the ideal sensing range is at least twice the communication range. However, hidden and exposed nodes complicate the issue.

Node A's sensing range of $R_{S_A} \geq R_{I_A} + R_{C_C}$ ensures it never transmits while C is transmitting, thus avoiding collisions at B. However, it also cause A to defer while C is transmitting to a node outside of A's interference range, such as Node D. This results in underutilization of the medium. However, the possibility of increased collisions may be traded for higher network utilization by decreasing the sensing range. However, if the sensing range is decreased too much, the higher collision rate lowers network throughput. This situation is illustrated in Figure 1.2. Deferrals are

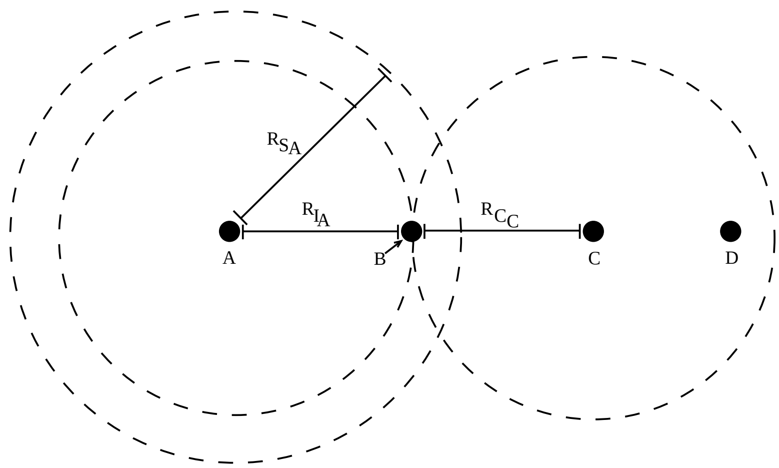


Figure 1.1 Determining Sensing Range

the number of times a packet is not transmitted due to a busy network. Deferrals are considered unnecessary if the deferred packet would not have caused any collisions if it had been transmitted. To maximize network throughput, one must determine the ideal sensing range of the network.

1.2 Problem and Significance

Since the cost of a collision is higher than the cost of a deferral, most implementations of 802.11 focus on reducing collisions. For this reason, it is common for the sensing range to be twice as large as the communication range. Such a large

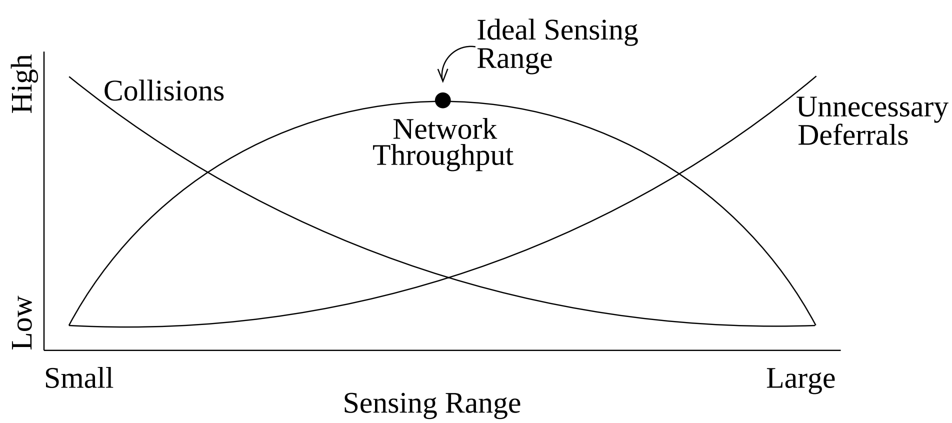


Figure 1.2 Ideal Sensing Range

sensing range can greatly reduce network efficiency [XS01], however, this result was obtained using a pedagogical example. It is not known what significance a large sensing range has on more typical multi-hop network topologies.

Since IEEE 802.11 is a very common protocol, it would be desirable to use the protocol in multi-hop networks. However, if 802.11 CCA inefficiencies are as serious as indicated in [XS01], they must first be addressed. Although CCA improvements would most benefit CSMA/CA based protocols such as 802.11, non-CSMA/CA based protocols would also stand to benefit because they too must sense the medium for a signal of some sort.

This research potentially benefits the US Air Force because if current multi-hop networks are using non-ideal sensing ranges, then a change in a single variable in the multi-hop protocol could increase network throughput. Determining these CCA issues is the focus of this study.

1.3 Research Goals

This research intends to first determine the magnitude of IEEE 802.11 CCA inefficiencies in a multi-hop environment. Next, it determines what network factors affect ideal sensing range. This information is used to set the sensing range to maximize network throughput.

1.4 Thesis Organization

This chapter contains a brief overview of the subject area and states the goals and direction of the research. Chapter 2 reviews current literature and research on multiple access methods, wireless MAC protocols, CSMA, problems of applying CSMA to a wireless network, and methods to overcome these problems. Chapter 3 presents the methodology used to accomplish this research including the system definition, evaluation techniques and experimental design. Chapter 4 presents the

research results and analysis. Finally, Chapter 5 summarizes and presents the conclusions of this research effort.

II. Literature Review

This chapter presents background information on medium access control (MAC) protocols and their application to wireless multi-hop ad-hoc networks. It presents techniques used by MAC protocols to permit multiple access to a medium and also describes the ALOHA and Carrier Sense Multiple Access (CSMA) protocols. The chapter describes challenges facing CSMA based protocols such has hidden and exposed nodes as well as issues associated with clear channel assessment (CCA). Protocols which improve upon CSMA are described including CSMA with collision avoidance (CSMA/CA), Multiple Access with Collision Avoidance (MACA), MACAW, and IEEE 802.11. A brief description of non-CSMA based protocols is also given.

2.1 Multi-Hop Ad-Hoc Networks

Computer networks have become a critical part of the United State's and the U.S. military's infrastructure. In fact, the US military's reliance on computer networks extends to virtually every aspect of war. Although the military is currently heavily reliant upon a wired medium, wireless networks are increasingly being implemented where a wired medium is either impractical or too expensive.

The simplest wireless networks are common within or around office buildings and consist of access points connected to a wired network. Wireless nodes communicate with the access points. Ad-hoc wireless networks on the other hand, do not rely on access points. In an ad-hoc network, wireless nodes communicate directly with each other. For example, such a network would allow communication between several laptops in a remote location. Since no infrastructure is required, aside from the nodes themselves, ad-hoc networks are relatively cheap.

The simplest ad-hoc networks are fully-connected, meaning all nodes can directly communicate with each other. As ad-hoc networks become larger, it may not be possible for a node at one network extreme to communicate with a node at the

other. For such nodes to communicate, one or more nodes must relay the message. A network having relay capability is called a multi-hop ad-hoc network, or simply a multi-hop network. Every node in a multi-hop network can potentially serve as a router.

Multi-hop network protocols have two key design issues. First, the dynamic routing protocol determines a node's neighbors and the best route to other nodes. Second, the medium access control (MAC) protocol provides efficient access to the wireless medium. This study focuses on the latter design issue.

2.2 MAC Protocols

Wireless networks are similar to wired networks since all nodes share a common communications medium. As in a wired network, if two wireless nodes transmit at the same time, their signals will interfere and result in a collision. The task of the MAC protocol is to avoid collisions and to resolve collisions when they do occur. In addition, the MAC protocol must do this in a fair and efficient manner. The MAC protocol is contained within the datalink layer of the Open Systems Interconnection (OSI) reference model as specified by the International Standards Organization [Int84].

2.2.1 Multiple Access Methods. There are many MAC protocols with each utilizing a different technique to control channel access. These methods can be reduced to five general categories:

1. Space Division

   Most MAC protocols are designed based on the assumption that the wireless nodes are equipped with omni-directional antennas. An omni-directional antenna transmits and receives energy equally in all directions. An alternative is to use directional antennas. The strategy used by space division protocols is to limit the area of transmission to allow simultaneous transmissions

that would not be possible with omni-directional antennas. Directional antenna MAC protocols have the ability to improve overall network throughput [KSV00]. However, directional antennas can be costly and are not practical for many devices. The remaining methods focus on omni-directional antennas.

2. Random Access

   One method to control channel access is to simply not control it at all. Nodes using such protocols transmit without regard to other node activity. If a collision is detected, the packet is rescheduled. This type of access method was first implemented with the ALOHA System as explained in Section 2.3.1 [Abr70]. Such protocols are quite simple but relatively inefficient. They form the basis for more advanced protocols such as 802.11 and Ethernet.

3. Partition Time

   Another method to achieve multiple access is to partition time by dividing it into slots. This method is known as Time Division Multiple Access (TDMA) [Skl88]. In this case, each node only transmits in its assigned slot. At any given time, only one node is allowed to transmit thus collisions are eliminated. Fixed assignment TDMA can be wasteful though because slots are assigned to a node whether or not that node has a packet to transmit. TDMA is commonly used for cellular services.

   A variation of fixed assignment TDMA is Random-TDMA (RTDMA) [CH75]. This technique dynamically allocates time slots to specific nodes. Thus, any node may transmit during any slot. This method is generally more efficient than a pure random access scheme since the slots force packets to completely overlap rather than partially overlap. This effectively reduces the number of collisions by half [Abr77].

4. Partition Frequency

A fourth method to provide common channel access is to partition the available transmit frequency band using Frequency Division Multiple Access (FDMA). Using this method, each system node is assigned a different communication frequency [Skl88]. By doing this, nodes may transmit simultaneously without interference. Thus, this method subdivides a channel into several sub-channels.

This method does have some drawbacks. A frequency sub-band can only be assigned to one node, which limits the number of system nodes to a function of the system's bandwidth. It can also lead to wasted bandwidth since a particular frequency sub-band is unused if a node is not transmitting.

5. Spread Spectrum

   A spread spectrum system utilizes bandwidth in excess of the minimum bandwidth necessary to send the information [Skl88]. Spreading is typically accomplished by means of a binary code. At the receiver, the same code is used to de-spread the signal. A unique code may be assigned to each node thus allowing for multiple access. This technique is referred to as Code Division Multiple Access (CDMA).

   The two common spread spectrum techniques are direct-sequence (DSSS) and frequency-hopping (FHSS). In a DSSS system, a narrow-band signal is transformed into a wide-band signal with a spreading code [Skl88]. Any other node with the spreading code may de-spread the signal. This technique allows multiple nodes to send simultaneously and offers side benefits such as security and jamming resistance.

   A FHSS system transmits narrow-band information but frequently changes the transmission frequency [Skl88]. The hopping pattern is maintained in the code signal thus any other node with the code signal may properly receive the transmission. Like DSSS, FHSS provides the benefits of security and jamming resistance in addition to multiple access.

2.3 *Early Wireless Protocols*

2.3.1 ALOHA. One of the first wireless MAC protocols, ALOHA, was implemented in 1971 at the University of Hawaii [Abr70]. The system concept is very simple and of the five general categories, falls into the random access category. The system consists of the following modes [Skl88]:

1. *Transmission mode.* Nodes transmit any time they have a packet waiting for transmission, encoding the transmissions with an error detection code.
2. *Listening mode.* After a message transmission, a node listens for an acknowledgment (ACK) from the receiver. Transmissions from different nodes will sometimes conflict. In such cases, errors are detected and the transmitting nodes receive a negative acknowledgment (NAK).
3. *Retransmission mode.* When a NAK is received, the messages are simply retransmitted. Of course, if the colliding users were to retransmit immediately, they would collide again. Therefore, the nodes retransmit after a random delay.
4. *Timeout mode.* If after a transmission the node does not receive either an ACK or NAK within a specified time, the node retransmits the message.

This simplicity of control comes at the expense of channel capacity. Statistical analysis has shown that the "pure" ALOHA channel can only achieve a maximum normalized throughput of $\frac{1}{2e} = 0.184$ [Abr77]. This low throughput is the result of high collision rates since nodes transmit without regard for each other's activity.

To improve ALOHA's performance, Slotted ALOHA was introduced [Abr77]. Slotted ALOHA uses a RTDMA scheme. A sequence of synchronization pulses is transmitted to all system nodes. A "slot" is defined as the time between synchronization pulses and are of the same duration as a packet transmission. When a node has a packet to transmit, the transmission is scheduled to start at the next slot boundary. In this way, conflicting packets overlap completely rather than partially and as

a result, the rate of collisions is reduced by half. This has the effect of doubling the normalized throughput of the ALOHA protocol to $\frac{1}{e} = 0.368$ [Abr77].

2.3.2 CSMA. ALOHA's poor performance is due to its high collision rate. One method to reduce collisions is based on a method used by airplane pilots. Each pilot first listens to the radio to ensure no one else is transmitting before transmitting their own message. In networks, this protocol is referred to as Carrier Sense Multiple Access (CSMA). Since CSMA allows nodes to access the medium one at a time but does not assign specific slots, it is essentially a RTDMA system [KT75].

A node using CSMA behaves much like a node using ALOHA except that it first senses the medium before transmitting. If another nearby node is transmitting, the medium is sensed as busy and the node defers, i.e., it refrains from transmitting until a later time. If the medium is sensed as free, the node transmits.

There are two general CSMA categories: persistent and non-persistent. When persistent CSMA senses a busy medium, it waits until the channel is idle and then immediately transmits. However, if multiple nodes are waiting, they will transmit at the same time with a collision resulting. To avoid this, persistent CSMA can be generalized to p-persistent. If p-persistent CSMA senses an idle channel, the node transmits with probability p. Otherwise, it defers with probability $1 - p$. If the channel is sensed as busy, the node waits until the channel is idle and then operates as previously described. Thus, persistent CSMA is equivalent to p-persistent CSMA where $p = 1$ [KT75]. Using a lower p value reduces the chances of collision when the channel becomes idle. Non-persistent CSMA differs from p-persistent in that a packet is always rescheduled if the channel is sensed as busy. If the channel is sensed as idle, the node always transmits. However, since rescheduling is a randomized process, there is low probability of multiple nodes transmitting when the channel becomes idle. This leads to fewer collisions and reaches a maximal channel capacity of 0.815 when all nodes are within range of all other nodes [KT75]. This led to

CSMA based protocols becoming popular within the network industry. The most popular CSMA protocol is Ethernet which uses a CSMA with Collision Detection (CSMA/CD) protocol [PD00]. Since wireless nodes cannot simultaneously send and receive, CSMA/CD is not used in wireless applications.

2.4 CSMA Performance Problems

2.4.1 Hidden/Exposed Nodes. CSMA suffers a fundamental problem associated with wireless networks. As network size increases, the assumption that all nodes are within the communication range of all other nodes is invalid. This results in what are known as hidden and exposed nodes. A hidden node scenario is illustrated in Figure 2.1. The communication and sensing ranges, which are equally sized in this example, are represented by the solid circles. Figure 2.1 shows node A transmitting to node B. Node C has a packet to transmit to node D. Following the CSMA protocol, node C senses the medium and since node A is beyond C's sensing range, it does not detect a transmission and continues its transmission to node D. Node A's and node C's transmissions overlap at node B causing a collision. This collision results from the fact that A's transmission is *hidden* from C.

Now consider exposed node case illustrated in Figure 2.2. Here, node B is transmitting to node A. Node C has a packet to transmit to node D. Following the CSMA protocol, node C first senses the medium. Since C is within the transmission range of B, C senses B's transmission and defers its transmission to a later time. However, C could have transmitted without a resulting collision. This is due to the fact that each signal only overlaps at their respective transmitting nodes; each target node receives a clear signal. In the exposed node case, a collision does not occur. However, bandwidth is not fully utilized.

2.4.2 Clear Channel Assessment (CCA). Hidden and exposed node problems are exacerbated by the method which wireless nodes use to sense the medium.

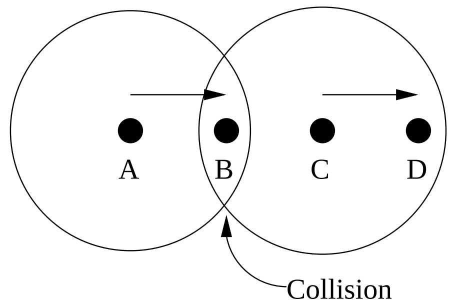


Figure 2.1 Hidden Node Scenario

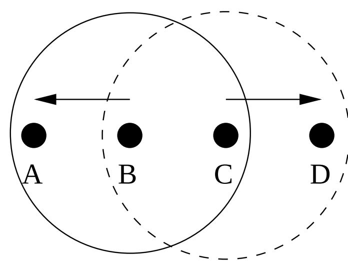


Figure 2.2 Exposed Node Scenario

The process of determining whether the channel is busy or not is called Clear Channel Assessment (CCA). The CCA process measures the amount of RF energy at the receiver. If the energy level is above a certain threshold, the medium is considered busy, otherwise it is considered idle. This is illustrated in Figure 2.3. This figure shows signal degradation as the distance from the transmitter increases. If a node receives a signal with a strength greater than the communication threshold, it can reliably receive and interpret that transmission. If the received signal strength is lower than the communication threshold, but greater than the sensing threshold, the node is aware that another node is transmitting but is unable to decode the signal (communicate). If the received signal strength is less than the sensing threshold, the node is unable to differentiate between a signal and noise.

Assuming uniform signal decay rates, the thresholds may be mapped to ranges as shown in Figure 2.4. In this figure, node A is transmitting. Node B is within A's communication range therefore B is able to successfully receive and interpret A's

signal. Node C is between A's communication and sensing ranges, therefore, it is able to sense A's transmission but it is unable to decode it.

Not shown in the figures is the interference range. This is not set by the protocol but is a product of protocol, network topology, and environmental factors. Therefore, it cannot be clearly defined. It is the range at which a node's transmission no longer causes interference at another node. The sensing range is typically larger than the communication range [SK99]. In addition, the sensing range is usually larger than the interference range which means that the transmission can be sensed at a range beyond which it may cause interference.

For example, in IEEE 802.11 based WaveLAN wireless radios, the interference range and sensing range are more than two times the size of the communication range [XS01]. A larger sensing range means that a node with a packet to transmit could sense the medium as busy and defer when it could have transmitted without interference. A larger interference range means that a node could sense the medium as free and transmit but still cause interference at another node beyond the transmitting node's communication range.

In a fully connected network, the ideal sensing range is one that minimizes collisions as Figure 2.5 illustrates. Node A must not transmit when another node within A's interference range (R_{I_A}) is receiving data, e.g., node B. In a worst case, node B is located on the interference range border as illustrated. Node C represents the furthest node from B that can communicate to B. Thus, B is within

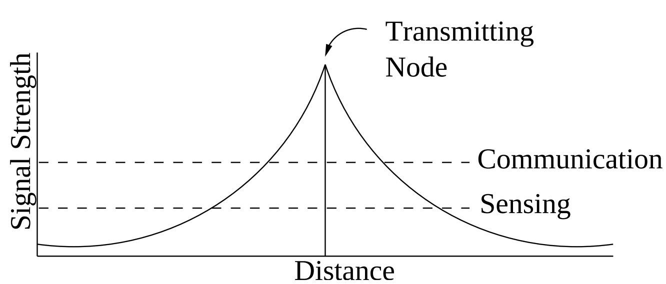


Figure 2.3 CCA Power Thresholds

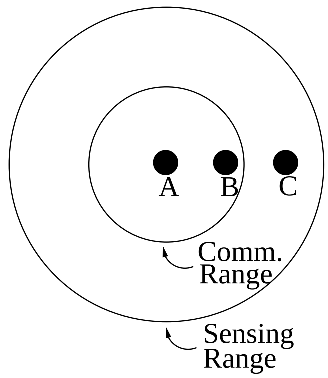


Figure 2.4 CCA Power Ranges

the communication range of C (R_{C_C}). From this representation, it can be seen that to minimize collisions between packets from A and C that simultaneously arrive at B, A must have a sensing range $R_{S_A} \geq R_{I_A} + R_{C_C}$ such that A can detect (sense) that C is transmitting. Since a node's interference range is at least equal to the communication range, the ideal sensing range is at least twice the communication range. However, hidden and exposed nodes complicate the issue.

Node A's sensing range of $R_{S_A} \geq R_{I_A} + R_{C_C}$ ensures it never transmits while C is transmitting, thus avoiding collisions at B. However, it also cause A to defer while C is transmitting to a node outside of A's interference range, such as Node D. This results in underutilization of the medium. However, the possibility of increased collisions may be traded for higher network utilization by decreasing the sensing range. However, if the sensing range is decreased too much, the higher collision rate lowers network throughput. To maximize network throughput, one must determine the ideal sensing range of the network.

It is clear that these CCA issues are closely related to the hidden and exposed node problems. In a wireless network where every node can sense every other node, these problems have only minor impact. However, in networks containing hidden and exposed nodes, such as multi-hop networks, these problems cause serious per-

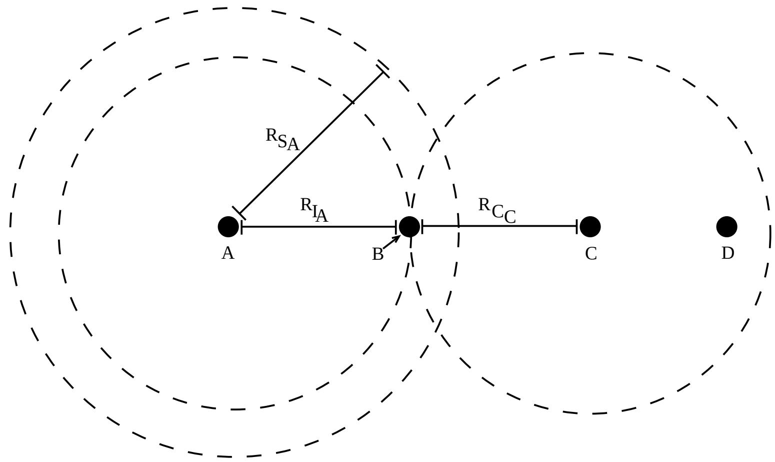


Figure 2.5 Determining Sensing Range

formance degradation. For these reasons, pure CSMA is inappropriate for multi-hop wireless ad-hoc networks.

2.5 Overcoming CSMA Performance Problems

Hidden and exposed nodes illustrate the fundamental problem with CSMA. Collisions only matter when they occur at a receiving node. They do not matter if they occur at a transmitting node. However, CSMA uses carrier sensing to determine whether or not a node is transmitting. What is really needed is a method to determine whether or not a node is receiving. This section looks at some of the methods to improve CSMA by focusing on what is happening at the receiving rather than the transmitting node.

2.5.1 RTS/CTS Protocols. CSMA with Collision Avoidance (CSMA/CA) extends CSMA by introducing a handshaking routine between nodes before exchanging data. CSMA/CA was originally implemented by Apple for the Localtalk network [Kar90]. Multiple Access with Collision Avoidance (MACA) uses CSMA/CA as its fundamental protocol [Kar90]. The basic idea behind MACA is for the sender to stimulate the receiver into outputting a short frame so nearby nodes can detect this

transmission and defer transmitting for the duration of the upcoming (larger) data frames [Tan96].

MACA works as follows. If node A has a packet to transmit to node B, node A first transmits a Request-to-Send (RTS) packet. This packet contains the source node, the destination node, and the data length. If node B receives the RTS packet and is currently not deferring to another transmission, it transmits a Clear-to-Send packet (CTS) back to A. Upon receiving the CTS packet, node A immediately transmits the data packet to B. Any other node sensing A's RTS packet defers from transmitting for enough time to allow B to respond with a CTS packet. Any other node that senses B's CTS packet knows that B is about to receive data and defers from sending for enough time to allow B to receive the data.

Using the hidden node scenario in Figure 2.1, node C does not sense the RTS from node A since it is out of range. However, node C does sense B's CTS packet. Thus C knows that a node nearby is receiving data and defers from transmitting long enough to allow B to receive the data. In the exposed node scenario in Figure 2.2, node C would sense node B's RTS packet but would not sense node A's CTS packet. Thus, node C knows that either node A is down and not responding or out of range. Either way, node C is free to transmit. Thus, MACA effectively handles these situations but it does not completely solve the hidden/exposed node problems. In particular, it is still possible for RTS and CTS packets to collide. Since these packets are much smaller than a data packet, the possibility of collision is reduced, but they still can cause a significant reduction is throughput.

One improvement to MACA is MACAW [BDSZ94]. MACAW introduces an acknowledgment (ACK) frame after each successful data frame and requires nodes to use carrier sensing before transmitting RTS frames. It also has a separate backoff algorithm for each data stream rather than one for each node, thus improving fairness of the protocol. Finally, MACAW allows nodes to exchange congestion information to improve system performance [Tan96].

MACA/MACAW methods achieve good results and serve as a basis for the IEEE 802.11 protocols. IEEE 802.11 can function using two access methods, the point coordination function (PCF) and the distributed coordination function (DCF). The PCF is for use with static access points thus not suitable for ad-hoc networks. With DCF, a node desiring to transmit senses the medium. If the medium is busy, it defers. If the medium is idle for a specified amount of time, the node transmits. The sending and receiving nodes may optionally perform a RTS/CTS handshake to reduce collisions. Once the data frame is received, the receiving node checks the packet for errors. If it was received error free, the node sends an acknowledgment packet to the transmitting node. If the sending station does not receive an acknowledgment, it retransmits the packet until it receives an acknowledgment or gives up after a certain number of attempts.

The success of 802.11 has resulted in it becoming the de-facto standard in wireless communications. However, IEEE 802.11 has serious performance problems in multi-hop networks primarily due to deficiencies in DCF. There are four specific problems in 802.11 when used in a multi-hop environment [XS01].

- The hidden node problem still exists. Although the 802.11 standard addresses this problem with the RTS/CTS handshake, such a scheme cannot eliminate all collisions due to hidden nodes. This problem is aggravated in multi-hop networks since such networks will always have hidden nodes.
- The exposed node problem is not addressed at all by the 802.11 standard. In a multi-hop environment, the exposed node problem can create a greater degradation in performance than the hidden node problem.
- Many common implementations of the 802.11 standard have sensing and interference ranges much larger than the communication range. This intensifies hidden and exposed node problems and severely degrades performance in a multi-hop network.

- The binary exponential backoff scheme used by DCF induces unfairness since it favors the latest successful node. While this is true for all network environments, it is especially severe in multi-hop networks.

2.5.2 Busy-Tone Protocols. Because of CSMA's inherent weaknesses in wireless networks, many alternatives have been proposed. The first was proposed by Kleinrock and Tobagi who published a study of CSMA protocols [KT75]. They subsequently published a companion paper proposing the idea of busy tones [TK75]. The Busy Tone Multiple Access (BTMA) protocol uses a central base station that transmits an out-of-band signal (busy tone) while receiving data. Nodes defer transmission while the busy tone is sensed. Since BTMA uses centralized access points, it is not appropriate for ad-hoc networks. However, the idea has served as a basis for ad-hoc busy tone protocols.

The Dual Busy Tone Multiple Access protocol (DBTMA) works by splitting the channel into two sub-channels [HT99], one data channel and one control channel. In addition to RTS and CTS control packets, the DBTMA protocol adds a transmission busy tone (BT_t) and a receive busy tone (BT_r). Before a source node sends a packet, it first tries to sense the BT_r signal. If it does sense the BT_r signal, it defers, otherwise it transmits an RTS packet to the destination node. When the target node receives the RTS packet, it tries to sense the BT_t signal. If it does, it defers, otherwise is begins transmitting the BT_r signal and transmits a CTS packet to the source node. When the source node receives the CTS packet, it simultaneously transmits a BT_t signal and data packet to the target node. When the source node finishes sending the data packet, it stops sending the BT_t signal. When the destination node stops receiving the data packet it stops sending the BT_r. DBTMA outperforms MACA throughput by about 100% and achieves a maximum throughput of 0.7 [HT99]. This protocol eliminates all collisions of data packets and greatly reduces the chances of RTS/CTS packets colliding.

The Wireless Collision Detect (WCD) protocol is very similar to DBTMA [GL00]. WCD eliminates the use of a RTS/CTS handshake, using only a sending and receiving busy tone to avoid collisions. Simulations of WCD show maximum normalized throughputs of up to 0.97 are achievable in a fully connected network; multi-hop network analysis was not provided. Achieving such high throughput is dependent on using the optimal packet size which may vary across networks. However, in all cases studied, WCD shows a significant improvement over 802.11 and HIPERLAN [GL00].

The Europe Telecommunication Standardization Institute (ETSI) created the HIPERLAN wireless protocol which uses a MAC protocol called Elimination Yield Non-pre-emptive Priority Multiple Access (EY-NPMA). Like WCD, this protocol does not use an RTS/CTS handshake. The protocol incorporates node priority allowing higher priority packets to have access to the network faster than low priority packets. Nodes of the same priority resolve who accesses to the channel through a random length elimination tone followed by a random length yield time. The protocol throughput approaches 0.85 in a fully connected network. As hidden nodes are introduced, throughput degrades, achieving 0.6 with 5 hidden node pairs [FGB96].

2.6 Summary

This chapter contains background information relating to MAC protocols and their application to wireless networks. It describes methods that various protocols may use to achieve multiple access to a common channel. The early wireless protocols, ALOHA and CSMA, are also described. CSMA's performance problems related to hidden and exposed nodes as well as clear channel assessment are described in detail. Following this, the chapter provides an overview of more recently proposed methods to overcome these problems.

III. Methodology

This chapter presents research goals and the methodology used to reach them. The system of study and parameters affecting the system are specified. In addition, factors that are varied in the system to determine the effects of sensing range in an ad-hoc network are described. Lastly, the chapter presents the experimental design used for the research.

3.1 Problem Definition and Research Goals

A large sensing range can have a significant effect on throughput [XS01]. However, no studies using other than pedagogical examples were discovered. Further, no published studies were found that determine the effect of static sensing ranges on multi-hop networks or determine what an ideal sensing range of a network should be.

Therefore, the research goals are as follows:

1. Determine the performance impact of sensing threshold levels on network throughput specifically for multi-hop networks.
2. Determine primary factors affecting ideal sensing threshold levels.
3. Propose MAC protocol improvements that take advantage of these factors.

Due to the nature of the CSMA protocol, it is expected that the presence of both hidden and exposed nodes will be the primary factor affecting protocol efficiency. The presence of hidden and exposed nodes are in-turn determined by network topology and the communication range of each node. The severity of the effect of hidden and exposed nodes is a function of network traffic. When these factors combine to create several hidden and exposed nodes, and the load is high enough to make them significant, we hypothesize that a large sensing range will cause a significant number of unnecessary deferrals which in-turn leads to lower throughput. By decreasing the

sensing range, the number of unnecessary deferrals will decrease, thus improving network throughput.

3.2 Approach

The first objective, measuring the performance impact of current threshold levels on multi-hop networks, indicates just how important sensing range is to system performance. If the ideal range only creates a small improvement in performance, it may not be worthwhile to modify a network to incorporate new protocols or introduce the additional overhead such protocols may require. However, given preliminary data shown in other studies we expect sensing range to have a significant effect [XS01].

To determine the second objective, we create a series of networks. Each network varies in size, topology, and traffic load. For each network, we submit an offered workload, vary the node sensing range and observe network performance. From this information we determine which sensing range is ideal for each network and determine which factors have the greatest influence on ideal sensing range. Methods a node can use to determine optimal sensing range are then explored.

3.3 System Boundaries

This research focuses on the physical layer and Medium Access Control (MAC) component of the data link layer of wireless multi-hop networks. All network nodes run the same protocols using the same settings. Thus, the system under test (SUT) is the MAC and physical layers of all network nodes. The component under test (CUT) is the sensing threshold (ST) level specified in the MAC protocol. System boundaries are illustrated in Figure 3.1.

There are additional methods that could be implemented at the MAC and physical layers to solve the problems discussed in Section 3.1. For example, transmission signal strength can be varied dynamically to decrease exposed node problems. However, investigation of power control methods is beyond the scope of this

research. Instead, the research focuses on solving the problem mentioned by varying the sensing threshold only.

3.4 System Services and Possible Outcomes

The MAC and physical network layers provide service to the higher level network layers. They take a packet from the link control layer as input and transmit the packet across the medium. These layers also listen to the medium for incoming packets which are received and passed up to the link control layer.

For any network node, the MAC layer is in one of two states, either it has packets to transmit or it does not. If the MAC layer does not have any packets to transmit, it will not attempt to gain channel access. If it does have a packet to transmit, it will contend for channel access. Thus, channel contention results in one of four outcomes: (1) the node transmits and the transmission does not result in a collision at any node, (2) the node transmits and the transmission causes a collision at one or more nodes, (3) the node does not transmit, but if it had, a collision would have resulted, or (4) the node does not transmit, but if it had, a collision would not have resulted. Outcomes one and three are desired while two and four are undesired.

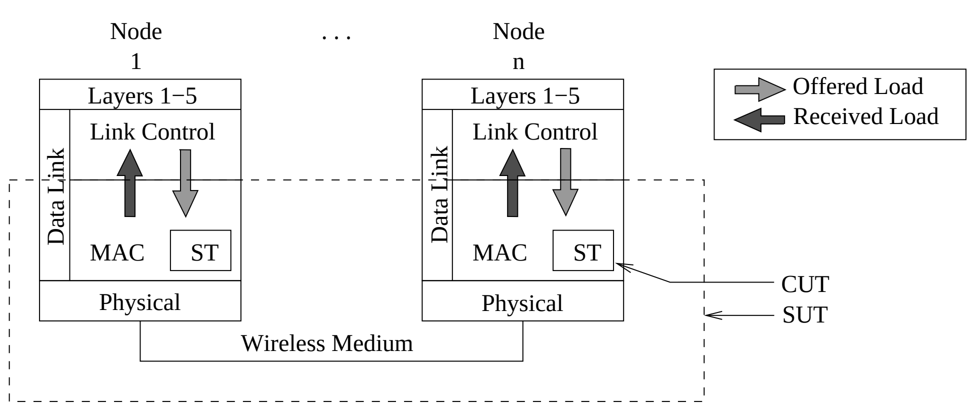


Figure 3.1 System Boundaries

3.5 *Performance Metrics*

The following metrics are used to measure the system:

- Average Network Throughput - Throughput S is defined by

$$S = \frac{b}{t} \tag{3.1}$$

where b is the number of successfully transmitted bits and t is the period of observation in seconds. This measures the average number of data bits transmitted per second. Network throughput measures the number of bits passed to the link layer, excluding MAC layer control bits.

This higher-is-better metric is chosen since it provides a measure of network efficiency. An efficient network transmits multiple packets simultaneously when possible, resulting in higher throughput. For a fully connected network, only one node may transmit at a time and S has a maximum value equaling the node transmission rates. Network configurations that take advantage of spatial reuse yield higher throughput rates.

- Average Collisions Per Packet - Average collisions per packet $\bar{C}$ is defined as

$$\bar{C} = \frac{\sum_{all\, i} c_i}{P} \tag{3.2}$$

where c_i is the number of collisions suffered by the i^{th} packet, and P is the total number of transmitted packets. A collision is counted when the transmission of another packet causes interference. A single packet can collide with multiple packets during transmission. It is possible for two packets to collide, yet one or both are successfully received due to the capture effect of radio receivers. Such collisions are counted in this statistic.

- Average Deferral Slots Per Packet - Average deferral slots per packet $\bar{D}$ is defined as

$$\bar{D} = \frac{\sum_{\mathrm{All}\, n} d_n}{P} \tag{3.3}$$

where d_n is the total number of deferral slots at the n^{th} node and P is the total number of transmitted packets. A deferral occurs whenever a node refrains from transmitting a packet due to a busy medium. This results in the node backing-off randomized number of slots. This statistic records the average number of back-off slots per second. A deferral can occur multiple times for a single packet if the medium remains busy when the node exits the back-off state.

3.6 System Parameters

Network performance is affected by a number of parameters which are divided into two categories: system and workload.

- System Parameters
  - Antenna Type - A transmitter antenna can be directional or omni-directional. This research uses omni-directional antennas only.
  - Number of nodes - The number of network nodes, N, measures the total number of nodes trying to gain access to the medium. The nodes can be considered system "customers" and the goal is to service as many customers as fast as possible.
  - Node Topology - The physical relationship between nodes is a determinant in the ability of the MAC protocol to take advantage of spatial reuse.
  - Environmental topology - This includes physical obstruction between nodes, including walls, hills, or the Earth itself. Obstructions influence the decay rate of a wireless signal.

  - Signal Strength - This is the wireless signal transmitted power and is a significant factor in node communication range. It also partly determines the existence of hidden and exposed nodes.
  - Routing Protocol - The ad-hoc network routing protocol determines a routing path for each packet. The routing protocol can be a significant source of overhead on an ad-hoc network. The routing protocol resides in the network layer.
  - MAC Protocol - This protocol is used by each network node to negotiate medium sharing. The MAC protocol lies within the data link layer and consists of two main sub-parameters:
    - Sensing Threshold - This is the energy level at which a node considers the medium busy. The effect of this factor is the component under study (CUT).
    - Other MAC options - This category includes all options that may be varied at the MAC layer. These options include the back-off method used and the amount of time a node listens to the channel before transmitting. It also includes the use of additional collision avoidance methods such as a RTS/CTS handshake.
- Workload Parameters
  - Offered Load (bits/sec) - This parameter is the rate at which packets arrive at the MAC layer of each node.
  - Packet size (bytes) - Packet size can be either constant or variable. When constant, packet size is specified in bytes. When variable, average packet size as well as a distribution by which the packet size is modeled is usually specified.

3.7 System Factors

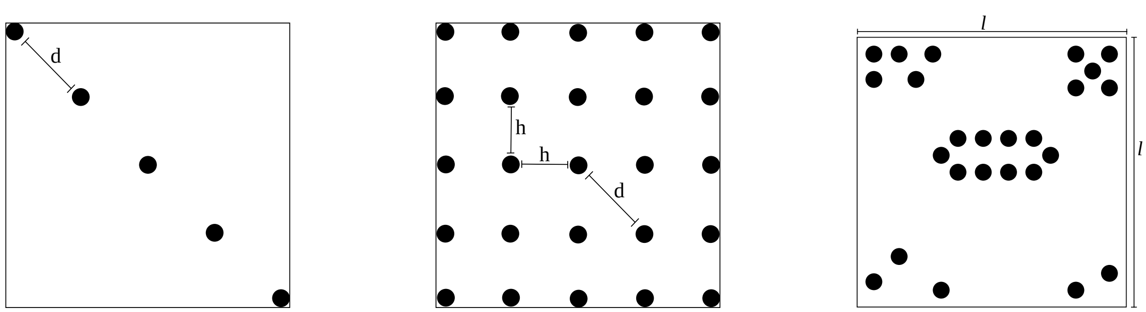
From the list of parameters above, factors are selected as those most likely having a significant influence on network performance. All other parameters are set equivalently on all nodes and not varied.

1. Network Size and Topology - This study uses two 25 node networks and one 5 node network. One of the 25 node networks is arranged in a 5 x 5 matrix with equal row and column spacing between the nodes (Figure 3.2b). This creates a uniformly distributed network. The second network is designed to resemble a more realistic network topology and consists of several node clusters (Figure 3.2c). Each cluster could represent, for instance, a location at a remote military installation. The five node network is arranged in a linear fashion as shown in Figure 3.2a.

   To measure the effect of introducing hidden and exposed nodes, the distance between nodes is varied. For the 5 node and 25 node uniform network, the distance between diagonally adjacent nodes is defined as d. This study uses a commonly used power setting of 1 mW which results in a communication range of about 250 meters. As shown in Table 3.1, four sizes for each network topology are obtained by varying d such that $d = \frac{R_c}{x}$ where $x = \{1, 2, 3, 4\}$. The horizontal distance between nodes, h, is determined from the diagonal distance and l is the total length of the network area. Networks of size $d = \frac{R_C}{4}$ result in every node within communication range of every other node, i.e., a fully connected network. Networks of size $d = R_C$ are very large and each node can only communicate with its nearest neighbors. Sizes $d = \frac{R_c}{2}$ and $d = \frac{R_C}{3}$ provide intermediate degrees of hidden and exposed nodes. The clustered network was similarly expanded to fill a total area equal to l^2 as shown in Table 3.1. The relative distance between each node is maintained for each size.

Table 3.1 Uniform Network Sizes

d	$h = \sqrt{\frac{d^2}{2}}$	$l = 4h$
$R_c = 250.0$ m	176.77 m	707.08 m
$\frac{1}{2}R_C = 125.0$ m	88.39 m	353.56 m
$\frac{1}{3}R_C = 83.3$ m	58.90 m	235.60 m
$\frac{1}{4}R_C = 62.5$ m	44.19 m	176.76 m



(a) 5 Node Network

(b) 25 Node Uniform Network

(c) 25 Node Clustered Network

Figure 3.2 Network Topologies

2. Sensing Range - Sensing range (R_s) is a function of communication range (R_c). The following levels are used for the sensing range: $2R_c$, $1R_c$ and $\frac{1}{2}R_c$. For a standard communication range of 250 m, the given R_S levels equate to 500 m, 250 m and 125 m. The simulation uses a 2-ray path loss model for signal attenuation [GS]. Using this model, the received packet power,P_{rcvd}, that has propagated the distance, D, is determined by

$$P_{rcvd} = P_{in\,band} \cdot P_{loss} \cdot G_{tx\,ant} \cdot G_{rx\,ant} \tag{3.4}$$

where $G_{tx\,ant}$ and $G_{rx\,ant}$ are transmitting and receiving antenna gains which are set to 1 for this research. $P_{in\,band}$ is the in-band transmit power which is set to 0.24 mW, and P_{loss} is path loss determined by [GS]:

$$P_{loss} = 4\left(sin\left(\frac{2\pi}{\omega D}\right)\right)^2\left(\frac{\omega^2}{16\pi^2 D^2}\right) \tag{3.5}$$

where $\omega = 0.12433\,m$ is the wavelength. Using (3.4) and (3.5) and setting D to the desired sensing range results in P_{rcvd}, the desired sensing thresholds, measured in Watts, shown in Table 3.2.

3. Offered Load - Offered Load, λ in bps, is modeled using a Poisson process and set based upon the network transmission rate. Network capacity is defined as μ with units of bps. Each node has a low, medium and high setting defined as follows: Low $= \frac{\mu}{N}(0.1)$, Medium $= \frac{\mu}{N}(0.5)$, and High $= \frac{\mu}{N}(0.9)$, where N is the number of nodes on the network. For this study, a transmission rate of 1.0

Table 3.2 Sensing Threshold Levels

Sensing Range (m)	Sensing Threshold (W)
$2R_c = 500$	1.5946E-14
$R_c = 250$	2.5253E-13
$\frac{1}{2}R_c = 250$	3.8776E-12

Mbps is used, resulting in load levels shown in Table 3.3. Although this rate was chosen due to model limitations, it does not affect research results since transmission rate is not a factor determining ideal sensing range.

3.8 Evaluation Technique

This research uses simulation as the method of evaluation. This method is selected because analytic modeling would be too complex for the system as specified and several simplifying assumptions would be necessary; these assumptions would greatly reduce the value of the model. Direct measurement is not feasible as it would require additional software running on the nodes which could affect node performance. Furthermore, the hardware needed for such modeling is not available.

The simulation model is validated by conducting tests on a 4-node network using a linear topology. This network is simple enough that packet transmissions can be scheduled in such a way that network performance is predictable using a combination of expert and statistical analysis. The predicted performance is compared with actual performance.

3.9 Workload

For this study, only the MAC and Physical layers of each node are modeled since they are the focus of this research. Therefore, the workload generated is passed directly to the MAC layer, as opposed to first passing through OSI network layers one through five. Each node independently generates a workload based upon a Poisson distribution with mean arrival rate, λ, a factor (see Section 3.7).

Table 3.3 Load Levels per Node

Level	λ, 25-nodes (bps)	λ, 5-nodes (bps)
Low $=\frac{\mu}{N}(0.1)$	4,000	20,000
Medium $=\frac{\mu}{N}(0.5)$	20,000	100,000
High $=\frac{\mu}{N}(0.9)$	36,000	180,000

Packets are generated with a constant size of 256 bits. This size is chosen because MAC protocols usually use reservation protocols (such as RTS/CTS) or fragmentation when data sizes become large. Since these are not being modeled, a smaller packet size is chosen. Furthermore, a smaller packet size results in increased medium contention, the MAC phase this study is interested in. However, packet size is expected to have an insignificant effect on ideal sensing range; this is verified during the study.

The IEEE 802.11 protocol is used as the MAC layer protocol. This protocol was chosen since it is widely available and broadly used. The optional use of RTS/CTS control packets is not simulated. The MAC settings used for all nodes is shown in Table 3.4. The values shown are either specified by the 802.11 protocol or commonly used in 802.11 implementations. Normally, the destination of each packet is set by the application layer. Since layers one through five are not being modeled, the destination is set during packet generation. The destination is randomly chosen from among all nodes within a slight overestimation of a source node's communication range. If the randomly chosen destination is greater than 300 meters from the source, another destination is randomly chosen. This process repeats until the randomly chosen destination is less than 300 meters from the source. This was done to approximate routing protocol effects which generally prevents nodes from transmitting to an out of range node. This allows generation of more accurate throughput data since when a node transmits to an out of range node, it retransmits the packet seven times before giving up.

3.10 Experimental Design

A full factorial experimental design is used for this study. Each network topology of Figure 3.2 requires 36 runs, resulting in a total of 108 runs. The 36 runs performed on each network topology are specified in Table 3.5.

Table 3.4 MAC Settings Used for all Nodes

Parameter	Value
Data Rate	1.0 Mbps
CDMA Mode	Direct Sequence
Retry Limit	7
Buffer Size	256,000 bits
Bandwidth	22,000 Khz
Min Frequency	2,402 Mhz
Altitude	1.0 m
Modulation	bpsk

To obtain a measure of throughput variability for a given run, the simulation time is divided into 500 statistic collection "bins". Throughput S is determined for each bin according to (3.1). Deferrals are recorded in a similar fashion by dividing the simulation time into 500 bins and determining the average deferral slots per packet for each bin in accordance with (3.3). Collisions are calculated on a per packet basis per (3.2). However, given the large number of packets created during a simulation, 500 packets are randomly sampled to obtain the collision statistic. The sample size was chosen after estimating collision variability in preliminary runs.

Collected data has an accuracy of $\pm$ 5% with 95% confidence. Preliminary runs are conducted to determine throughput and collision rate variability. It was observed that data from all runs fell well within the desired confidence boundaries after about 120 s of simulation time. Therefore, 120 s is used for the simulation time. Furthermore, every run stabilized within 10 seconds. Therefore the first 10 seconds of simulated data is considered "transient" and discarded prior to metric calculation. All runs are replicated three times.

3.11 Summary

This chapter presents the research goals which are to determine the performance impact of sensing range on network throughput, determine the primary fac-

Table 3.5 Experimental Runs for Each Network Topology

Run	Size, d	Sensing Range, R_s	Load, λ
1	$R_C/4$	$2R_c$	Low
2	$R_C/4$	$1R_c$	Medium
3	$R_C/4$	$\frac{1}{2}R_c$	High
4	$R_C/4$	$2R_c$	Low
5	$R_C/4$	$1R_c$	Medium
6	$R_C/4$	$\frac{1}{2}R_c$	High
7	$R_C/4$	$2R_c$	Low
8	$R_C/4$	$1R_c$	Medium
9	$R_C/4$	$\frac{1}{2}R_c$	High
10	$R_C/3$	$2R_c$	Low
11	$R_C/3$	$1R_c$	Medium
12	$R_C/3$	$\frac{1}{2}R_c$	High
13	$R_C/3$	$2R_c$	Low
14	$R_C/3$	$1R_c$	Medium
15	$R_C/3$	$\frac{1}{2}R_c$	High
16	$R_C/3$	$2R_c$	Low
17	$R_C/3$	$1R_c$	Medium
18	$R_C/3$	$\frac{1}{2}R_c$	High
19	$R_C/2$	$2R_c$	Low
20	$R_C/2$	$1R_c$	Medium
21	$R_C/2$	$\frac{1}{2}R_c$	High
22	$R_C/2$	$2R_c$	Low
23	$R_C/2$	$1R_c$	Medium
24	$R_C/2$	$\frac{1}{2}R_c$	High
25	$R_C/2$	$2R_c$	Low
26	$R_C/2$	$1R_c$	Medium
27	$R_C/2$	$\frac{1}{2}R_c$	High
28	R_C	$2R_c$	Low
29	R_C	$1R_c$	Medium
30	R_C	$\frac{1}{2}R_c$	High
31	R_C	$2R_c$	Low
32	R_C	$1R_c$	Medium
33	R_C	$\frac{1}{2}R_c$	High
34	R_C	$2R_c$	Low
35	R_C	$1R_c$	Medium
36	R_C	$\frac{1}{2}R_c$	High

tors affecting the ideal range and to suggest ways this information can be applied to MAC protocol improvements. These goals are met by simulating three network topologies. A full factorial experimental design is used in which network size, sensing range, and applied load are varied.

IV. Results and Analysis

This chapter summarizes simulation results obtained in this study. Detailed results and raw data are presented in Appendix A. This chapter analyzes the results in light of the goals and hypothesis of this study.

4.1 Results

Mean throughput results from this study are presented in Table 4.1 and Figures 4.1 through 4.3. Throughput data shows that a sensing range of twice the communications range ($2R_c$) outperforms the other sensing ranges in almost all configurations. For size $d = \frac{R_C}{4}$ networks, sensing ranges of size $2R_c$ and R_c perform equivalently. This is expected since the R_c range already encompasses all nodes. The only case where $2R_c$ does not maximize throughput occurs in the clustered network, size $d = R_C$, at a 0.9 normalized load. In this configuration, a range of R_c gives statistically better performance yet the improvement is small at less than 1%.

The mean collision data in Table 4.2 and Figures 4.4 through 4.6 shows how increased sensing range does indeed reduce the number of collisions. In all cases, a larger sensing range results in fewer or a statistically equivalent number of collisions.

Table 4.3 and Figures 4.7 through 4.9 show the effects of sensing range on deferral slots. In almost every configuration, a smaller sensing range increased average deferrals slots per packet.

ANOVA analysis of throughput results are contained in Tables 4.4 through 4.6. ANOVA results show that all factors have a significant impact on throughput performance. The significance of each factor varies depending upon network topology. For the uniform network (Table 4.4) the load (L) and sensing range (C) account for 61% of the variation. This figure increases to 74% when 2nd-order effects are included. However, for the clustered network (Table 4.5) the sensing range is half as significant as in the uniform network. Here, load and size (S) are the most significant

Table 4.1 Mean Throughput (bits/sec)

Network Size	Load	Uniform Network			Clustered Network			5-Node Network		
		Sensing Range			Sensing Range			Sensing Range		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	100,292	100,186	99,815	100,419	99,868	99,303	99,904	100,064	69,939
4d	**Medium**	251,943	251,736	111,404	250,559	250,378	124,334	243,932	243,876	136,796
4d	**High**	251,809	251,799	122,050	250,263	250,222	124,300	243,706	243,893	183,731
3d	**Low**	98,122	97,491	93,543	98,931	98,556	94,505	99,988	99,542	42,395
3d	**Medium**	239,527	222,387	80,314	240,612	229,939	82,276	241,339	229,007	42,827
3d	**High**	239,553	225,052	80,485	240,598	229,841	82,159	241,341	229,158	42,920
2d	**Low**	95,863	92,690	81,856	97,944	95,904	84,666	100,267	72,136	37,089
2d	**Medium**	174,727	108,287	76,954	208,016	128,178	72,601	229,331	136,048	36,835
2d	**High**	180,630	107,536	76,957	209,823	127,859	72,477	228,903	135,827	36,882
1d	**Low**	99,558	99,548	99,941	99,282	99,300	99,203	99,805	75,590	26,124
1d	**Medium**	312,512	255,245	134,052	390,111	381,988	243,481	197,275	177,036	26,124
1d	**High**	312,569	254,696	134,100	532,849	545,646	287,010	197,627	177,278	26,236

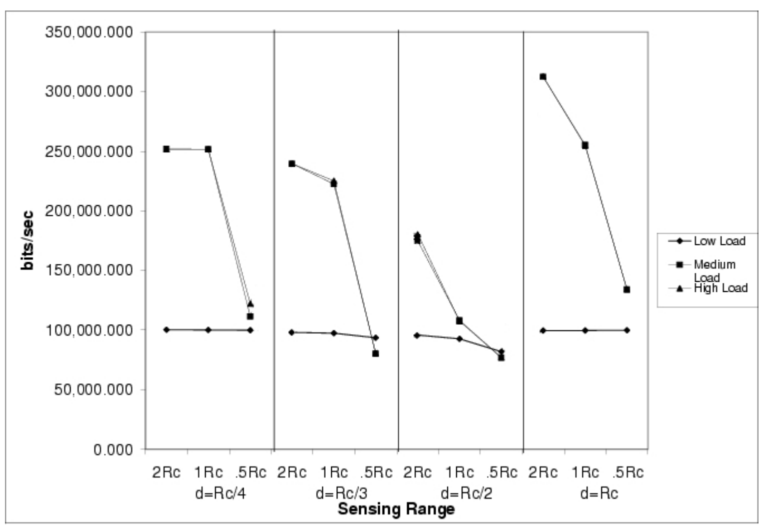


Figure 4.1 Throughput - Uniform Network (bps)

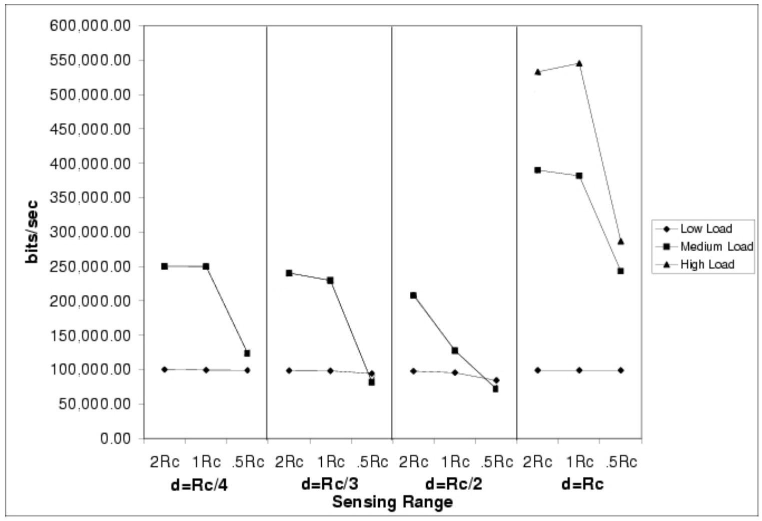


Figure 4.2 Throughput - Clustered Network (bps)

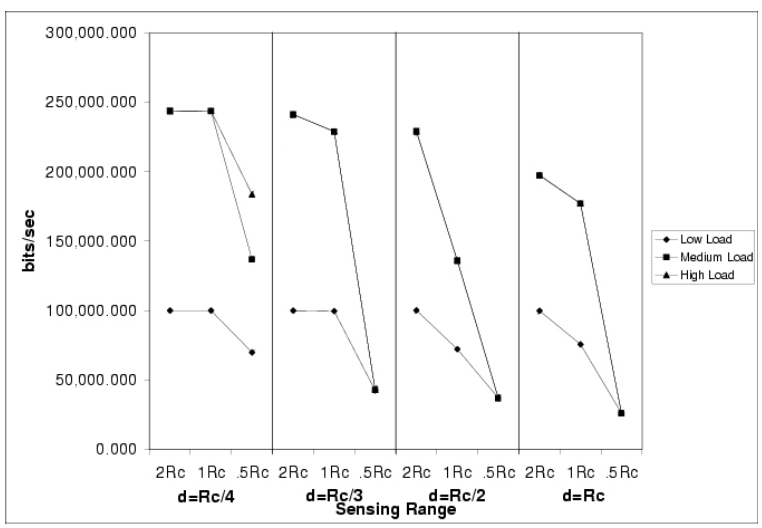


Figure 4.3 Throughput - 5-Node Network (bps)

Table 4.2 Mean Collisions (collisions/packet)

Network Size	Load	Uniform Network Sensing Range $2R_c$	$1R_c$	$\frac{1}{2}R_c$	Clustered Network Sensing Range $2R_c$	$1R_c$	$\frac{1}{2}R_c$	5-Node Network Sensing Range $2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	0.000	0.001	0.149	0.001	0.001	0.122	0.000	0.000	0.039
4d	**Medium**	0.139	0.147	0.966	0.130	0.156	0.864	0.044	0.044	0.041
4d	**High**	0.136	0.150	0.910	0.125	0.161	0.821	0.045	0.036	0.032
3d	**Low**	0.001	0.024	0.678	0.002	0.029	0.476	0.000	0.012	0.162
3d	**Medium**	0.115	0.182	1.588	0.118	0.188	1.582	0.041	0.066	0.152
3d	**High**	0.124	0.205	1.580	0.091	0.197	1.492	0.049	0.056	0.154
2d	**Low**	0.016	0.317	0.884	0.012	0.214	0.761	0.012	0.107	0.224
2d	**Medium**	0.133	1.089	2.109	0.124	0.818	1.880	0.082	0.171	0.203
2d	**High**	0.121	1.093	2.190	0.111	0.841	1.850	0.082	0.161	0.204
1d	**Low**	0.020	0.064	0.160	0.031	0.073	0.101	0.013	0.025	0.042
1d	**Medium**	0.439	0.942	1.441	0.397	0.751	1.042	0.083	0.094	0.041
1d	**High**	0.446	0.970	1.473	0.566	0.956	1.133	0.074	0.092	0.046

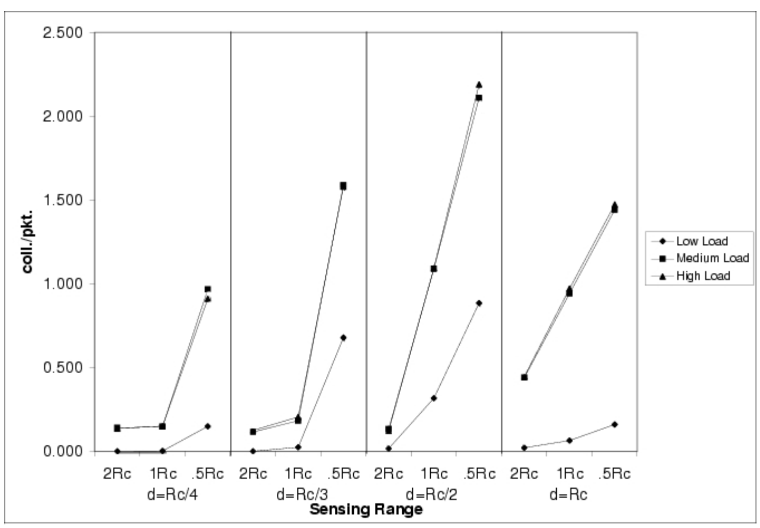


Figure 4.4 Collisions- Uniform Network (collisions/packet)

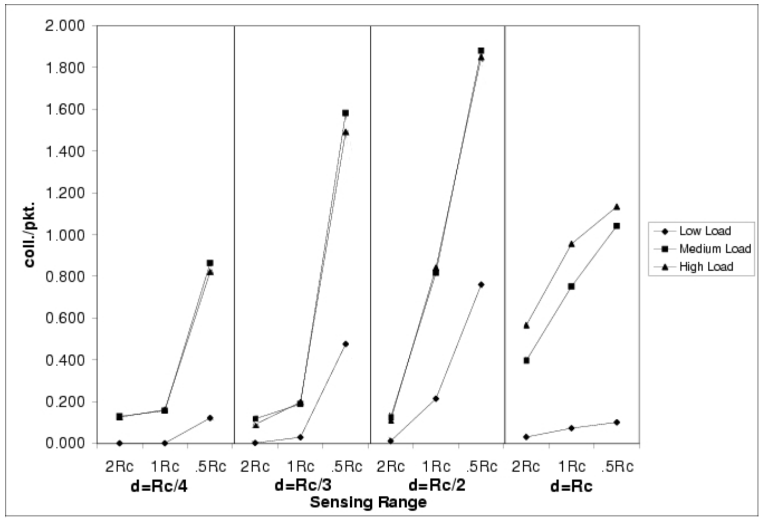


Figure 4.5 Collisions- Clustered Network (collisions/packet)

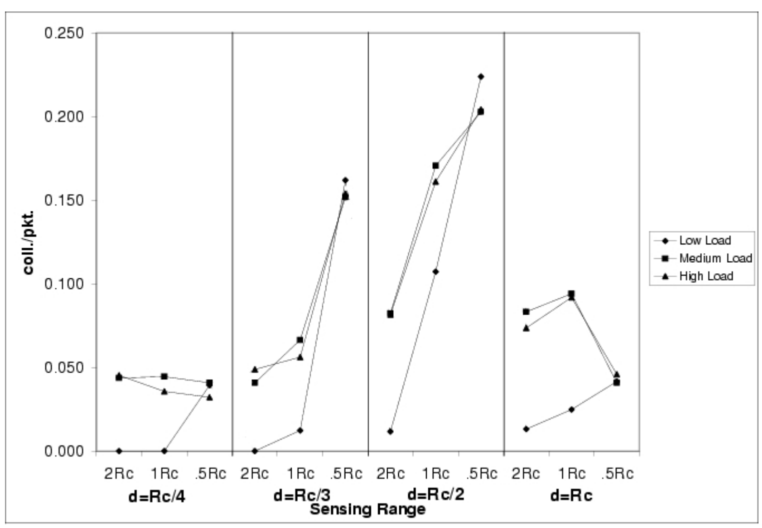


Figure 4.6 Collisions- 5-Node Network (collisions/packet)

Table 4.3 Mean Deferrals (slots/packet)

Network Size	Load	Uniform Network Sensing Range $2R_c$	$1R_c$	$\frac{1}{2}R_c$	Clustered Network Sensing Range $2R_c$	$1R_c$	$\frac{1}{2}R_c$	5-Node Network Sensing Range $2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	30	30	303	30	30	180	26	26	1,731
4d	**Medium**	1,577	1,536	10,577	1,617	1,618	9,767	94	93	1,270
4d	**High**	1,567	1,565	9,909	1,635	1,623	9,772	94	94	1,173
3d	**Low**	236	260	1,780	188	221	1,372	27	52	2,987
3d	**Medium**	3,089	4,340	13,392	2,929	3,816	13,289	93	331	2,970
3d	**High**	3,090	4,319	13,375	2,894	3,844	13,256	92	332	2,956
2d	**Low**	728	1,512	2,882	462	837	3,006	31	1,610	2,032
2d	**Medium**	5,834	10,642	10,424	4,111	9,005	13,784	262	1,155	2,049
2d	**High**	5,619	10,724	10,431	4,171	9,050	13,779	259	1,158	2,044
1d	**Low**	30	76	193	114	138	213	43	449	2,141
1d	**Medium**	1,593	3,116	2,005	834	1,169	2,805	452	565	2,141
1d	**High**	1,608	3,131	2,005	646	957	2,417	450	563	2,131

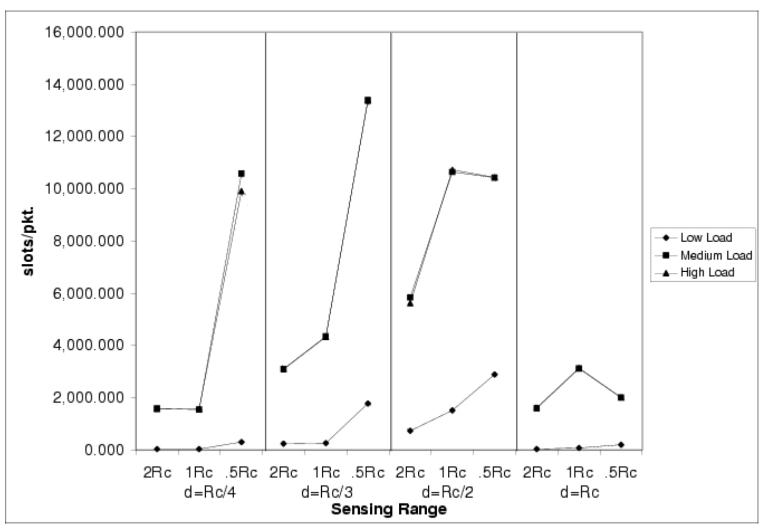


Figure 4.7 Deferrals- Uniform Network (slots/packet)

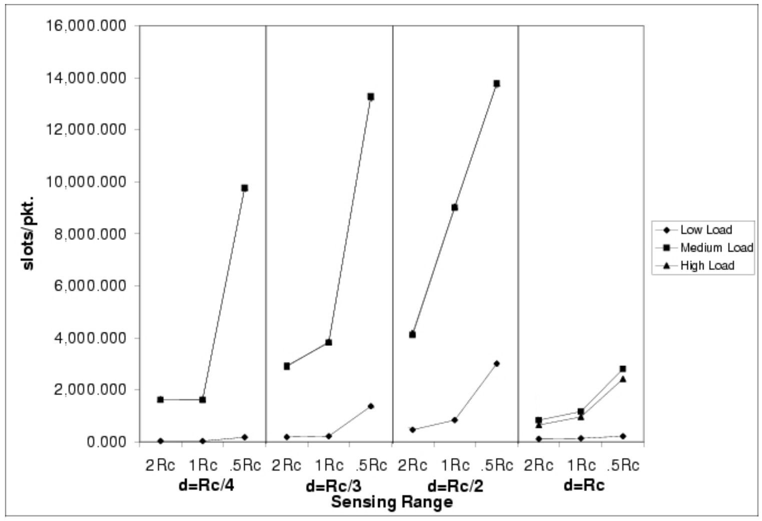


Figure 4.8 Deferrals- Clustered Network (slots/packet)

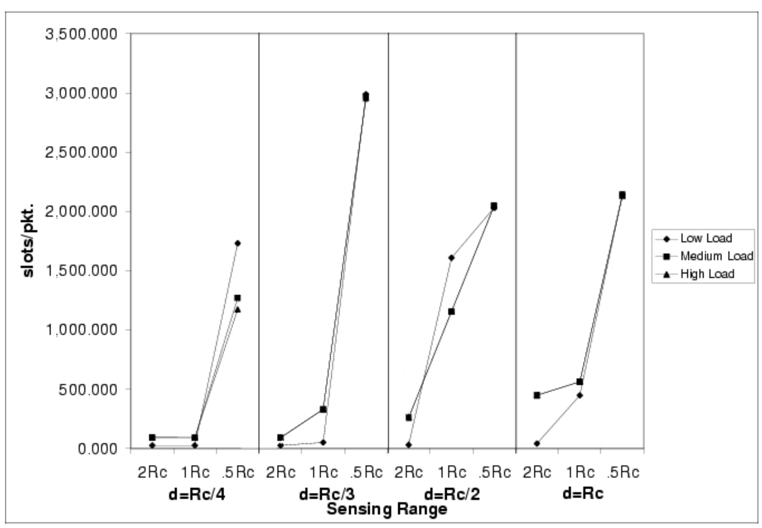


Figure 4.9 Deferrals- 5-Node Network (slots/packet)

and account for 58% of the variation and 75% of the variation when 2nd-order effects are included. The 5-node network (Table 4.6) more closely resembles the uniform network in that load and sensing range are the most significant factors, with sensing range alone accounting for 47% of the variation.

4.2 Analysis

This study hypothesized that as load and hidden/exposed nodes increase, a shorter sensing range would result in fewer deferrals. Fewer deferrals leads to higher throughput. Study results contradict this hypothesis. In all cases, a shorter sensing range increased average deferral slots per packet. This demonstrates that the benefits of simultaneous transmissions are small compared to the cost of collisions. When a collision occurs, not only is the time for the original transmission lost, but also the sending node must wait for a time-out period. This period is long enough for the receiving node to respond with an ACK. If the sending node fails to receive a response within the time-out period, it enters a backoff state where it must wait an average of 15.5 slots, assuming the previous transmission was successful. Slot time is defined by the IEEE 802.11 standard as 20 μs [IEE99].

Including physical layer overhead, data packets used in this study contained 537 bits and ACK packets contained 304 bits. At a transmission rate of 1.0 Mbps, it takes 537 μs and 304 μs respectively to transmit data and ACK packets. Thus, the minimum time to send a data packet and receive an ACK in return (send-ACK time) is 853 μs. This accounts for the transmission of the data and ACK packet, a 1 μs propagation time, plus half a slot time (10 μs) the receiving node must wait before responding with an ACK. The propagation time is intentionally overestimated. The actual average propagation time between nodes for the simulation is 0.5 μs. The one-half slot waiting time is known as a short inter-frame space (SIFS) and is defined by the IEEE 802.11 standard [IEE99]. In the case of a collision, after failing to receive an ACK in the expected 853 μs, the sending node backs-off an average

Table 4.4 Uniform Network ANOVA

Component	**% Var**	**Deg.Free**	**F-Computed**	**F-Table**
SST=	100	107		
Main Effects	77.3	7	125546.41	2.42
Size (S)	14.9	3	56613.16	3.01
Traffic (L)	31.0	2	176344.42	3.40
R_S **(C)**	31.3	2	178148.30	3.40
2nd-order Interactions	22.2	16	15750.86	2.09
SL	5.64	6	10685.42	2.51
SC	2.97	6	5620.01	2.51
LC	13.6	4	38545.29	2.78
3rd-order Interactions	0.517	12	489.38	2.18
Error	0.00211	24		

Table 4.5 Clustered Network ANOVA

Component	**% Var**	**Deg.Free**	**F-Computed**	**F-Table**
SST=	100	107		
Main Effects	73.9	7	201276.29	2.42
Size (S)	30.2	3	192128.53	3.01
Traffic (L)	28.3	2	269705.01	3.40
R_S **(C)**	15.4	2	146569.21	3.40
2nd-order Interactions	25.5	16	30391.81	2.09
SL	17.2	6	54789.83	2.51
SC	1.45	6	4619.72	2.51
LC	6.81	4	32452.92	2.78
3rd-order Interactions	0.561	12	891.71	2.18
Error	0.00126	24		

Table 4.6 5-Node Network ANOVA

Component	**% Var**	**Deg.Free**	**F-Computed**	**F-Table**
SST=	100	107		
Main Effects	82.8	7	196132.14	2.42
Size (S)	9.92	3	54770.54	3.01
Traffic (L)	25.4	2	210834.76	3.40
R_S **(C)**	47.5	2	393471.92	3.40
2nd-order Interactions	14.4	16	14940.81	2.09
SL	2.21	6	6096.96	2.51
SC	5.02	6	13857.41	2.51
LC	7.20	4	29831.70	2.78
3rd-order Interactions	0.03	12	3760.36	2.18
Error	0.00145	24		

of 15.5 slots which equals 310 μs. Thus, the total time cost for a collision is on average $853\,\mu\text{s} + 310\,\mu\text{s} = 1163\,\mu\text{s}$. Again, this assumes the previous transmission was successful.

If a simultaneous transmission occurs, the time to send a data packet and receive an ACK is saved in addition to the 2.5 slots (50 μs) that separate transmissions. The 2.5 slot time is the DCF inter-frame space (DIFS) as defined in the IEEE 802.11 standard [IEE99]. This totals 903 μs. Thus, two simultaneous transmissions save 78% of the cost of one collision. It takes at least three simultaneous transmissions to make up for the cost of a single collision. This means that unless a decreased sensing range significantly increases simultaneous transmissions, the costs outweigh the benefits.

The number of simultaneous transmissions occurring in a network can be estimated by observing network throughput. Assuming zero collisions, no other lost data, no simultaneous transmissions and at least one packet ready to transmit at all times, then 256 bits of data can be transmitted every 903 μs, this includes 853 μs send-ACK time plus a 50 μs DIFS time. This gives an upper bound of 283,499 data bits per second. When results show a throughput greater than this amount, it is assumed that a particular network is taking advantage of simultaneous transmissions. Note that a throughput value below this bound does *not* necessarily mean that simultaneous transmissions did not occur; only that a conclusion cannot be made on throughput data alone.

Observation of throughput results show that size $d = R_C$ configurations do surpass the calculated upper bound, indicating they are taking advantage of spatial reuse. The highest throughput among all configurations is 545,646 bps which occurs in the clustered network, size $d = R_C$, at a 0.9 normalized load. In this case, the sensing range is R_c. This implies there is a high occurrence of simultaneous transmissions. This configuration is the only configuration where a sensing range lower than $2R_c$ yields higher throughput. This is consistent with previous analysis

that a shorter sensing range is only beneficial if it significantly increases simultaneous transmissions.

Further evidence for this analysis is explained in Section 1.1 and Figure 1.1; to avoid collisions, a sensing range equivalent to the interference range of node A (R_{I_A}) plus the communication range of node C (R_{C_C}) is needed. A node's interference range is at least equal to its communication range. Thus, a sensing range of at least twice the communication range ($2R_c$) is expected to minimize collisions. This is borne out by the simulated collision data.

4.3 Additional experiments

If the interference range extends well beyond a node's communication range, then a sensing range greater than $2R_c$ could yield better results. To test this, simulations using sensing ranges of 2.5 and 3 times the communication range were considered. These studies were only performed on the uniform network. The results are shown in Tables 4.7 through 4.9. Both the $2.5R_c$ and $3R_c$ cases perform similarly. There is an upper limit on the benefit of sensing range size and no additional benefit is obtained by increasing the range beyond this. For smaller networks, this limit is reached simply because the network is a finite size. Once a sensing range encompasses all existing nodes, increasing its size has no effect. A limit is also incurred due to the effect of ambient background noise. Once a transmission's received power falls below the noise threshold, it cannot be distinguished from the noise. Therefore, a receiver simulation model does not accept packets having received power below the noise threshold. Thus, the lower sensing threshold limit equals the noise threshold.

Comparing the $3R_c$ and $2R_c$ throughput results in Tables 4.7 and 4.1 respectively, we see that a $2R_c$ sensing range slightly outperforms a $3R_c$ range in most cases. The exceptions are a $d = \frac{R_C}{2}$ and $d = R_C$ network size at 0.5 normalized load. However, these differences are small. Furthermore, the $3R_c$ and $4R_c$ studies were not replicated. Thus, confidence intervals were not obtained and we cannot

Table 4.7 $3R_c$ and $2.5R_c$ Mean Throughput (bits/sec)

Network Size	**Load**	**Sensing Range** $3R_c$	$2.5R_c$
4d	**Low**	99,825	100,481
4d	**Medium**	251,250	251,301
4d	**High**	251,532	251,380
3d	**Low**	97,237	98,171
3d	**Medium**	238,985	238,976
3d	**High**	239,223	239,484
2d	**Low**	95,914	95,772
2d	**Medium**	174,714	174,743
2d	**High**	179,131	179,394
1d	**Low**	99,837	99,301
1d	**Medium**	311,689	313,486
1d	**High**	311,759	311,615

Table 4.8 $3R_c$ and $2.5R_c$ Mean Collisions (collisions/packet)

Network Size	**Load**	**Sensing Range** $3R_c$	$2.5R_c$
4d	**Low**	0.002	0.002
4d	**Medium**	0.117	0.140
4d	**High**	0.127	0.155
3d	**Low**	0.000	0.000
3d	**Medium**	0.135	0.127
3d	**High**	0.122	0.122
2d	**Low**	0.022	0.024
2d	**Medium**	0.127	0.131
2d	**High**	0.107	0.140
1d	**Low**	0.026	0.028
1d	**Medium**	0.406	0.406
1d	**High**	0.419	0.389

Table 4.9 $3R_c$ and $2.5R_c$ Mean Deferrals (slots/packet)

Network Size	**Load**	**Sensing Range** $3R_c$	$2.5R_c$
4d	**Low**	30	30
4d	**Medium**	1,509	1,569
4d	**High**	1,588	1,593
3d	**Low**	238	238
3d	**Medium**	3,084	3,025
3d	**High**	3,081	3,067
2d	**Low**	690	734
2d	**Medium**	5,824	5,812
2d	**High**	5,720	5,969
1d	**Low**	30	31
1d	**Medium**	1,612	1,573
1d	**High**	1,593	1,586

say whether the values are statistically different. They do suggest though, that the sensing range resulting in the highest throughput is between 2 and 3 times the communication range, with most cases being closer to 2 times the communication range. Since $R_{S_{ideal}} = R_I + R_C$, the interference range of nodes in the study was between 1 and 2 times the communication range, with most cases being closer to 1 times the communication ranges. It also suggests that adjusting the sensing range to obtain greater throughput will only yield small improvements.

We also conducted studies varying the load distribution. These results are shown in Tables 4.10 through 4.12. These studies looked at a uniform network at a 0.5 normalized load. Table 4.10 shows results using normally distributed inter-arrival times. The normal distribution had a mean of 0.0128 s and a standard deviation of 1.0. Table 4.11 shows results using a Pareto distributed inter-arrival time. The Pareto distribution location parameter is 0.0128 and the shape parameter is 2.0. The shape value was chosen since it is commonly used in modeling networks. The location was chosen so that the distribution mean is 0.0128 seconds. Table 4.12 shows results for a uniform distribution where the minimum inter-arrival time is 0

seconds and the maximum inter-arrival time is 0.0256 seconds. This leads to a mean inter-arrival time of 0.0128 seconds.

The results indicate that the Pareto and uniform distributions are similar to the exponential inter-arrival time used in the study. The normalized distribution however shows instances where a R_c sensing range performed best and shows a $\frac{R_C}{2}$ sensing range performing equivalently to a $2R_c$ range. This suggests that the results obtained in this study may not be applicable to networks with normally distributed arrival patterns. However, this cannot be stated conclusively since the simulations were only run at a 0.5 normalized load on the uniform network and were not replicated.

Finally, we conducted a study to confirm our assumption that packet size has minimal effect on ideal sensing range. This study used a packet size of 1024 bits and the uniform network. All 36 runs, as depicted in Table 3.5, were replicated three times. Results are shown in Tables 4.13 through 4.15. Since the 1024 bit packet size is more efficient than a 256 bit packet size, throughput values are much higher for most configurations. However, the relative throughput performance of each sensing range is very similar to the 256 bit results. This confirms our assumption that packet size does not affect the ideal sensing range.

4.4 Summary

This chapter presents results indicating a lower sensing range does not lead to reduced deferrals even if there are several hidden/exposed nodes and the load is high enough to make them significant. Maximum throughput is usually obtained with the sensing range that minimizes collisions which is usually $2R_c$. However, there is one instance where a size R_C sensing range results in better throughput.

Table 4.10 Normally Distributed Load Results

Network Size	R_s	**Throughput (bits/sec)**	**Collisions (coll./pkt.)**	**Deferrals (slots/pkt.)**
4d	$2R_c$	15,905	0.000	17
4d	$1R_c$	16,066	0.000	21
4d	$\frac{1}{2}R_c$	15,469	0.002	22
3d	$2R_c$	15,234	0.000	77
3d	$1R_c$	15,609	0.002	89
3d	$\frac{1}{2}R_c$	15,309	0.002	77
2d	$2R_c$	15,665	0.000	157
2d	$1R_c$	14,995	0.013	160
2d	$\frac{1}{2}R_c$	14,823	0.009	163
1d	$2R_c$	15,957	0.002	19
1d	$1R_c$	15,703	0.002	20
1d	$\frac{1}{2}R_c$	15,456	0.000	26

Table 4.11 Pareto Distributed Load Results

Network Size	R_s	**Throughput (bits/sec)**	**Collisions (coll./pkt.)**	**Deferrals (slots/pkt.)**
4d	$2R_c$	250,066	0.063	531
4d	$1R_c$	248,900	0.081	585
4d	$\frac{1}{2}R_c$	105,093	0.939	11,018
3d	$2R_c$	223,408	0.061	2,722
3d	$1R_c$	188,493	0.229	4,545
3d	$\frac{1}{2}R_c$	79,717	1.546	13,467
2d	$2R_c$	169,497	0.170	5,866
2d	$1R_c$	107,813	1.074	10,614
2d	$\frac{1}{2}R_c$	77,359	2.197	10,358
1d	$2R_c$	312,776	0.437	1,566
1d	$1R_c$	254,896	1.037	3,116
1d	$\frac{1}{2}R_c$	133,603	1.476	2,008

Table 4.12 Uniform Distributed Load Results

Network Size	R_s	**Throughput (bits/sec)**	**Collisions (coll./pkt.)**	**Deferrals (slots/pkt.)**
4d	$2R_c$	251,038	0.138	1,600
4d	$1R_c$	251,268	0.166	1,583
4d	$\frac{1}{2}R_c$	110,911	0.915	10,640
3d	$2R_c$	238,808	0.096	3,136
3d	$1R_c$	221,473	0.194	4,311
3d	$\frac{1}{2}R_c$	80,356	1.572	13,324
2d	$2R_c$	174,573	0.153	5,839
2d	$1R_c$	107,813	1.074	10,614
2d	$\frac{1}{2}R_c$	77,359	2.197	10,358
1d	$2R_c$	312,776	0.437	1,566
1d	$1R_c$	254,896	1.037	3,116
1d	$\frac{1}{2}R_c$	133,603	1.476	2,008

Table 4.13 1024-bit Packet Throughput Results (bits/sec)

Network Size	**Load**	**Sensing Range**		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	99,969	100,436	99,816
4d	**Medium**	499,925	501,070	168,653
4d	**High**	550,070	550,129	178,972
3d	**Low**	98,369	97,321	96,082
3d	**Medium**	464,991	363,338	109,010
3d	**High**	513,185	430,049	110,189
2d	**Low**	89,883	85,868	84,956
2d	**Medium**	273,119	180,242	104,992
2d	**High**	282,872	179,171	104,681
1d	**Low**	100,115	100,041	99,122
1d	**Medium**	497,441	420,417	266,839
1d	**High**	618,619	460,410	251,350

Table 4.14 1024-bit Packet Collision Results (collisions/packet)

Network Size	**Load**	**Sensing Range**		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	0.000	0.000	0.045
4d	**Medium**	0.024	0.031	1.905
4d	**High**	0.140	0.140	1.895
3d	**Low**	0.000	0.005	0.322
3d	**Medium**	0.049	0.452	2.671
3d	**High**	0.093	0.323	2.663
2d	**Low**	0.007	0.116	0.193
2d	**Medium**	0.286	1.942	4.961
2d	**High**	0.265	1.965	5.051
1d	**Low**	0.007	0.013	0.028
1d	**Medium**	0.290	1.030	3.050
1d	**High**	0.681	1.857	3.980

Table 4.15 1024-bit Packet Deferral Results (slots/packet)

Network Size	**Load**	**Sensing Range**		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	5	5	15
4d	**Medium**	27	30	4,107
4d	**High**	405	394	3,898
3d	**Low**	30	35	50
3d	**Medium**	668	1,329	6,159
3d	**High**	857	1,217	6,116
2d	**Low**	187	175	174
2d	**Medium**	2,490	3,775	5,272
2d	**High**	2,418	3,811	5,316
1d	**Low**	7	11	18
1d	**Medium**	106	571	756
1d	**High**	634	1,130	933

V. Conclusions and Recommendations

This chapter summarizes this research. The research goals are restated and evaluated against the results. Finally, conclusions are drawn and recommendations for future work are presented.

5.1 Research Goals

The research goals were to determine the performance impact of sensing range on throughput in reference to multi-hop networks and to identify primary factors determining the ideal sensing range. The final goal was to use results to suggest improvements in current CSMA based wireless MAC protocols.

5.2 Results

Research results show that in every network configuration except one, a sensing range of $2R_c$ outperforms other range settings with respect to throughput. In the one instance where a range of R_c is best, the improvement over $2R_c$ is less than 1%. This suggests that the sensing range producing the fewest collisions usually yields the highest throughput. Exceptions to this occur if a shorter sensing range significantly increases spatial reuse. The increase in spatial reuse must be high enough to outweigh the cost of more collisions.

5.3 Conclusions

Based on research results, we conclude that using a static sensing range equal to twice the communication range provides maximal or near maximal throughput in most multi-hop networks. Due to the deficiencies of CSMA in a wireless environment, it is unlikely that multi-hop networks utilizing IEEE 802.11 will achieve the necessary spatial reuse with a smaller sensing range to realize significant throughput improvement. Thus, CCA inefficiencies are already minimized in many IEEE 802.11

implementations with a sensing range twice the communication range. Therefore, to eliminate these inefficiencies in multi-hop networks, protocols with high spatial reuse or non-CSMA based protocols should be considered.

These conclusions only apply within the assumptions made for this study. All nodes in the study use identical transmission power and physical obstructions do not exist between nodes. Thus, the interference range of all nodes are identical. Study results may not be applicable to networks with variable interference ranges.

5.4 Recommendations for Future Research

This research can be extended in many directions. The primary problem with a short sensing range is the high cost of collisions. Thus, if collisions can be reduced by another method, a shorter sensing range could allow for higher network utilization. Such methods could include the use of RTS/CTS protocols or error correction protocols.

This research shows that a shorter sensing range could be beneficial if the network utilizes spatial reuse. However, the degree of spatial reuse necessary to warrant a shorter sensing range is not identified by this study. Further simulation or an analytic model to determine this would be useful.

It would also be beneficial to extend this research toward multi-hop protocols that are not primarily CSMA based. Of particular interest would be protocols utilizing dynamic power transmission levels. Nodes using these protocols transmit with the minimum power necessary to reach their destination. This allows greater spatial reuse on the network, thus, in-line with the results of this study, a shorter sensing range could allow greater throughput.

Busy tone protocols allow receiving nodes to pro-actively announce their receiving status. Due to this major difference, results of this study may not be applicable to such protocols. This likewise applies to protocols operating in small physical areas

such as Blue-Tooth. It would be beneficial to determine if this research applies to these protocols as well.

5.5 Summary

This chapter concludes that a sensing range of twice the communication range provides maximal or near maximal throughput in most multi-hop networks. However, a shorter sensing range could be ideal in networks that take advantage of spatial reuse. Determining how much spatial reuse is necessary for this to be true is a subject for future research.

Appendix A. Data Analysis

This appendix presents all data collected during this study. For each network type, the mean throughput, collisions and deferrals values are presented. These tables are organized so all values for a specific network size and load are in the same row. This allows easy identification of the best sensing range. Next, the ANOVA of the throughput values for each network type is presented.

In order to perform ANOVA on the data, the following assumptions were made.

1. The effects of the various factors are additive.
2. Errors are additive.
3. Errors are independent of the factor levels.
4. Errors are normally distributed.
5. Errors have the same variance for all factor levels.

To verify the independence and normal distribution of errors, a residual versus response plot and a normal quantile-quantile plot were prepared for each network type. These plots are presented following the ANOVA results. For each residual versus resonse plot, no trend is evident in the data points which indicate that the errors are independent of the factors. For each normal quantile-quantile plot, the R^2 value was very high confirming the normality of errors.

After the ANOVA data, the raw results from the network simulation are presented. The **r** column is defined such that the 95% confidence interval can be described as $\bar{x} \pm r$, whereas r is a percentage value of the mean, $\bar{x}$.

A.1 Summarized Data - All Networks Topologies

Table A.1 Mean Throughput (bits/sec)

Network Size	**Load**	**Uniform Network**			**Clustered Network**			**5-Node Network**		
		Sensing Range			**Sensing Range**			**Sensing Range**		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	100,292	100,186	99,815	100,419	99,868	99,303	99,904	100,064	69,939
4d	**Medium**	251,943	251,736	111,404	250,559	250,378	124,334	243,932	243,876	136,796
4d	**High**	251,809	251,799	122,050	250,263	250,222	124,300	243,706	243,893	183,731
3d	**Low**	98,122	97,491	93,543	98,931	98,556	94,505	99,988	99,542	42,395
3d	**Medium**	239,527	222,387	80,314	240,612	229,939	82,276	241,339	229,007	42,827
3d	**High**	239,553	225,052	80,485	240,598	229,841	82,159	241,341	229,158	42,920
2d	**Low**	95,863	92,690	81,856	97,944	95,904	84,666	100,267	72,136	37,089
2d	**Medium**	174,727	108,287	76,954	208,016	128,178	72,601	229,331	136,048	36,835
2d	**High**	180,630	107,536	76,957	209,823	127,859	72,477	228,903	135,827	36,882
1d	**Low**	99,558	99,548	99,941	99,282	99,300	99,203	99,805	75,590	26,124
1d	**Medium**	312,512	255,245	134,052	390,111	381,988	243,481	197,275	177,036	26,124
1d	**High**	312,569	254,696	134,100	532,849	545,646	287,010	197,627	177,278	26,236

Table A.2 Mean Collisions (collisions/packet)

Network Size	**Load**	**Uniform Network**			**Clustered Network**			**5-Node Network**		
		Sensing Range			**Sensing Range**			**Sensing Range**		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	0.000	0.001	0.149	0.001	0.001	0.122	0.000	0.000	0.039
4d	**Medium**	0.139	0.147	0.966	0.130	0.156	0.864	0.044	0.044	0.041
4d	**High**	0.136	0.150	0.910	0.125	0.161	0.821	0.045	0.036	0.032
3d	**Low**	0.001	0.024	0.678	0.002	0.029	0.476	0.000	0.012	0.162
3d	**Medium**	0.115	0.182	1.588	0.118	0.188	1.582	0.041	0.066	0.152
3d	**High**	0.124	0.205	1.580	0.091	0.197	1.492	0.049	0.056	0.154
2d	**Low**	0.016	0.317	0.884	0.012	0.214	0.761	0.012	0.107	0.224
2d	**Medium**	0.133	1.089	2.109	0.124	0.818	1.880	0.082	0.171	0.203
2d	**High**	0.121	1.093	2.190	0.111	0.841	1.850	0.082	0.161	0.204
1d	**Low**	0.020	0.064	0.160	0.031	0.073	0.101	0.013	0.025	0.042
1d	**Medium**	0.439	0.942	1.441	0.397	0.751	1.042	0.083	0.094	0.041
1d	**High**	0.446	0.970	1.473	0.566	0.956	1.133	0.074	0.092	0.046

Table A.3 Mean Deferrals (slots/packet)

Network Size	Load	Uniform Network Sensing Range			Clustered Network Sensing Range			5-Node Network Sensing Range		
		$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$	$2R_c$	$1R_c$	$\frac{1}{2}R_c$
4d	**Low**	30	30	303	30	30	180	26	26	1,731
4d	**Medium**	1,577	1,536	10,577	1,617	1,618	9,767	94	93	1,270
4d	**High**	1,567	1,565	9,909	1,635	1,623	9,772	94	94	1,173
3d	**Low**	236	260	1,780	188	221	1,372	27	52	2,987
3d	**Medium**	3,089	4,340	13,392	2,929	3,816	13,289	93	331	2,970
3d	**High**	3,090	4,319	13,375	2,894	3,844	13,256	92	332	2,956
2d	**Low**	728	1,512	2,882	462	837	3,006	31	1,610	2,032
2d	**Medium**	5,834	10,642	10,424	4,111	9,005	13,784	262	1,155	2,049
2d	**High**	5,619	10,724	10,431	4,171	9,050	13,779	259	1,158	2,044
1d	**Low**	30	76	193	114	138	213	43	449	2,141
1d	**Medium**	1,593	3,116	2,005	834	1,169	2,805	452	565	2,141
1d	**High**	1,608	3,131	2,005	646	957	2,417	450	563	2,131

A.2 Uniform Network Data

Table A.4 Uniform Network Throughput ANOVA

Component	**% Var**	**Deg.Free**	**F-Computed**	**F-Table**
SST=	100	107		
Main Effects	77.3	7	125546.41	2.42
Size (S)	14.9	3	56613.16	3.01
Traffic (L)	31.0	2	176344.42	3.40
R_S **(C)**	31.3	2	178148.30	3.40
2nd-order Interactions	22.2	16	15750.86	2.09
SL	5.64	6	10685.42	2.51
SC	2.97	6	5620.01	2.51
LC	13.6	4	38545.29	2.78
3rd-order Interactions	0.517	12	489.38	2.18
Error	0.00211	24		

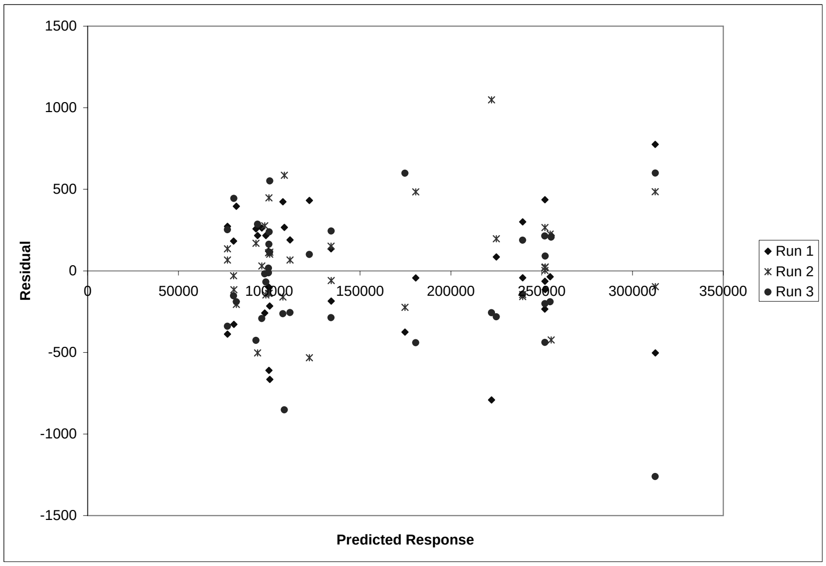


Figure A.1 Uniform Network Residual vs. Response Plot

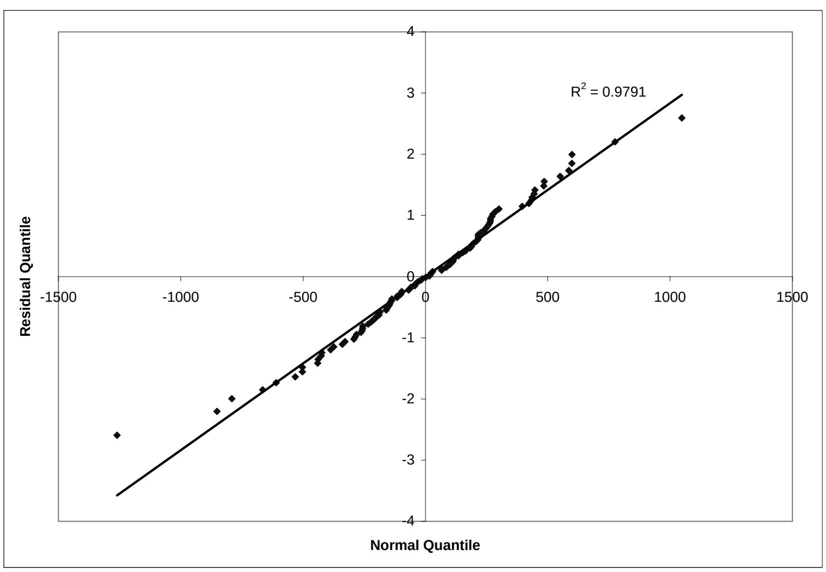


Figure A.2 Uniform Network Normal quantile-quantile Plot of Error

Table A.5 Uniform Network Simulation Results - Throughput (bits/sec)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%	
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	r
1	99,627.133	9,655.166	100,406.710	10,060.201	100,843.180	10,314.115	100,292.341	616.038	99,595.229	100,989.454	0.70%
2	251,829.030	5,682.889	251,966.740	5,607.484	252,034.427	5,595.116	251,943.399	104.669	251,824.955	252,061.843	0.05%
3	251,745.004	5,478.935	252,074.106	5,600.191	251,607.294	5,213.536	251,808.801	239.856	251,537.378	252,080.224	0.11%
4	99,970.241	10,890.025	100,287.673	10,186.481	100,299.344	10,112.576	100,185.752	186.730	99,974.448	100,397.057	0.21%
5	251,502.261	5,505.876	251,756.674	5,257.420	251,950.401	5,417.367	251,736.445	224.754	251,482.113	251,990.778	0.10%
6	252,235.157	5,162.130	251,801.021	5,401.473	251,359.883	5,582.927	251,798.687	437.641	251,303.449	252,293.925	0.20%
7	99,204.668	10,362.685	100,261.999	10,123.971	99,977.243	9,975.797	99,814.637	547.099	99,195.536	100,433.738	0.62%
8	111,593.873	8,317.107	111,470.168	8,651.268	111,148.067	8,361.050	111,404.036	230.143	111,143.605	111,664.467	0.23%
9	122,482.276	8,168.417	121,518.308	8,418.573	122,150.839	8,781.498	122,050.474	489.758	121,496.260	122,604.688	0.45%
10	98,338.731	10,489.411	97,974.617	10,183.916	98,053.975	10,689.738	98,122.441	191.469	97,905.773	98,339.109	0.22%
11	239,484.172	7,257.922	239,381.473	7,119.294	239,715.244	7,172.733	239,526.963	170.951	239,333.515	239,720.412	0.08%
12	239,852.954	7,161.746	239,395.478	6,709.145	239,409.482	7,262.872	239,552.638	260.176	239,258.222	239,847.054	0.12%
13	97,232.385	10,283.889	97,766.885	10,494.168	97,472.794	10,922.060	97,490.688	267.699	97,187.758	97,793.618	0.31%
14	221,595.915	7,437.295	223,435.157	7,493.661	222,130.416	7,477.863	222,387.163	946.119	221,316.528	223,457.797	0.48%
15	225,136.689	7,323.955	225,248.724	7,091.790	224,770.241	7,320.151	225,051.884	250.260	224,768.688	225,335.081	0.13%
16	93,759.300	8,215.935	93,040.408	8,192.276	93,829.322	8,430.882	93,543.010	436.671	93,048.870	94,037.150	0.53%
17	80,497.155	6,277.527	80,284.756	6,613.860	80,161.050	6,630.655	80,314.320	169.992	80,121.957	80,506.684	0.24%
18	80,156.382	6,946.847	80,368.782	6,488.160	80,928.957	7,023.682	80,484.707	399.120	80,033.060	80,936.354	0.56%
19	96,126.039	9,861.749	95,892.633	10,102.183	95,570.532	10,012.940	95,863.068	278.931	95,547.428	96,178.709	0.33%
20	174,352.152	13,545.846	174,503.866	14,111.904	175,325.456	13,031.650	174,727.158	523.665	174,134.575	175,319.740	0.34%
21	180,586.433	11,942.415	181,113.931	11,405.376	180,189.643	12,116.304	180,630.002	463.682	180,105.297	181,154.708	0.29%
22	92,947.046	9,109.540	92,858.352	8,931.030	92,263.166	9,626.247	92,689.521	371.888	92,268.690	93,110.352	0.45%
23	108,552.589	9,780.680	108,872.356	9,592.576	107,434.573	9,897.930	108,286.506	754.920	107,432.233	109,140.779	0.79%
24	107,959.737	9,699.859	107,376.222	10,018.653	107,273.523	9,935.663	107,536.494	370.119	107,117.665	107,955.323	0.39%
25	82,252.371	7,338.806	81,650.182	7,478.226	81,666.521	7,215.227	81,856.358	343.054	81,468.155	82,244.560	0.47%
26	76,566.594	6,780.892	77,089.424	6,543.108	77,206.127	6,831.049	76,954.048	340.581	76,568.644	77,339.452	0.50%
27	77,229.468	7,051.431	77,024.070	6,951.274	76,617.943	6,601.636	76,957.160	311.204	76,604.999	77,309.321	0.46%
28	99,459.081	10,441.846	99,669.147	9,393.038	99,545.441	10,904.263	99,557.890	105.585	99,438.409	99,677.370	0.12%
29	313,287.236	19,762.312	312,997.812	19,681.572	311,251.933	18,609.602	312,512.327	1,101.084	311,266.333	313,758.321	0.40%
30	312,066.521	19,544.567	312,472.648	18,262.664	313,168.198	20,937.742	312,569.122	557.139	311,938.660	313,199.584	0.20%
31	99,669.147	9,744.026	99,410.066	10,225.042	99,564.114	9,994.837	99,547.775	130.311	99,400.315	99,695.236	0.15%
32	255,460.832	15,451.675	254,821.298	14,932.077	255,451.495	14,582.868	255,244.542	366.569	254,829.730	255,659.354	0.16%
33	254,660.248	15,540.461	254,921.663	14,808.075	254,506.200	15,969.852	254,696.037	210.031	254,458.364	254,933.709	0.09%
34	99,839.533	9,781.484	99,804.522	10,060.956	100,180.306	9,685.906	99,941.454	207.592	99,706.542	100,176.366	0.24%
35	134,187.600	5,756.083	134,203.939	5,879.955	133,765.135	5,385.038	134,052.225	248.761	133,770.725	134,333.724	0.21%
36	133,914.515	5,787.737	134,040.554	5,673.394	134,343.982	5,449.665	134,099.684	220.755	133,849.876	134,349.492	0.19%

S.D. = Standard Deviation

Table A.6 Uniform Network Simulation Results - Collisions (collisions/packet)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%	
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	r
1	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	-
2	0.133	0.421	0.179	0.457	0.105	0.353	0.139	0.038	0.097	0.182	30.49%
3	0.160	0.448	0.105	0.353	0.142	0.439	0.136	0.028	0.104	0.167	23.30%
4	0.000	0.000	0.000	0.000	0.004	0.066	0.001	0.003	-0.001	0.004	196.00%
5	0.142	0.418	0.160	0.428	0.140	0.437	0.147	0.011	0.135	0.160	8.29%
6	0.147	0.422	0.140	0.427	0.164	0.470	0.150	0.012	0.136	0.164	9.37%
7	0.140	0.378	0.164	0.415	0.142	0.362	0.149	0.013	0.134	0.164	10.12%
8	0.978	0.819	0.928	0.793	0.993	0.793	0.966	0.034	0.928	1.005	4.02%
9	0.943	0.795	0.904	0.832	0.882	0.848	0.910	0.031	0.874	0.945	3.86%
10	0.000	0.000	0.002	0.047	0.000	0.000	0.001	0.001	-0.001	0.002	196.00%
11	0.096	0.337	0.105	0.372	0.144	0.393	0.115	0.026	0.086	0.144	25.18%
12	0.123	0.389	0.127	0.436	0.123	0.366	0.124	0.003	0.121	0.127	2.31%
13	0.028	0.166	0.020	0.139	0.024	0.153	0.024	0.004	0.019	0.029	20.57%
14	0.197	0.430	0.171	0.399	0.177	0.421	0.182	0.014	0.166	0.197	8.51%
15	0.225	0.468	0.190	0.455	0.199	0.441	0.205	0.018	0.184	0.226	10.06%
16	0.639	0.000	0.704	0.000	0.692	0.000	0.678	0.035	0.639	0.718	5.78%
17	1.595	0.901	1.613	0.894	1.556	0.949	1.588	0.029	1.555	1.621	2.08%
18	1.575	0.891	1.573	0.943	1.591	0.939	1.580	0.010	1.569	1.591	0.68%
19	0.018	0.131	0.024	0.153	0.007	0.081	0.016	0.009	0.006	0.026	62.36%
20	0.123	0.335	0.138	0.351	0.138	0.351	0.133	0.009	0.123	0.143	7.54%
21	0.127	0.346	0.116	0.334	0.120	0.352	0.121	0.006	0.115	0.127	5.15%
22	0.328	0.540	0.311	0.542	0.313	0.501	0.317	0.010	0.306	0.328	3.40%
23	1.066	0.732	1.118	0.813	1.083	0.785	1.089	0.027	1.059	1.119	2.78%
24	1.059	0.703	1.039	0.807	1.179	0.837	1.093	0.076	1.007	1.178	7.85%
25	0.921	0.909	0.884	0.954	0.847	0.902	0.884	0.037	0.842	0.926	4.76%
26	2.074	1.158	2.204	1.262	2.050	1.205	2.109	0.082	2.016	2.203	4.42%
27	2.217	1.217	2.168	1.333	2.184	1.257	2.190	0.025	2.162	2.217	1.27%
28	0.026	0.160	0.028	0.166	0.007	0.081	0.020	0.012	0.007	0.034	66.78%
29	0.464	0.658	0.427	0.665	0.427	0.614	0.439	0.021	0.415	0.463	5.53%
30	0.442	0.630	0.451	0.641	0.446	0.664	0.446	0.004	0.441	0.451	1.11%
31	0.063	0.253	0.066	0.257	0.063	0.270	0.064	0.001	0.063	0.066	2.23%
32	0.897	0.903	1.018	1.039	0.912	0.956	0.942	0.066	0.868	1.017	7.87%
33	0.965	0.954	1.020	1.020	0.926	0.970	0.970	0.047	0.917	1.024	5.51%
34	0.188	0.434	0.131	0.369	0.162	0.434	0.160	0.028	0.128	0.193	20.08%
35	1.363	1.217	1.545	1.370	1.416	1.325	1.441	0.093	1.336	1.547	7.34%
36	1.484	1.323	1.547	1.345	1.387	1.253	1.473	0.080	1.382	1.564	6.18%

S.D. = Standard Deviation

Table A.7 Uniform Network Simulation Results - Deferrals (slots/packet)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%	
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	r
1	30.240	6,415.912	29.567	2,443.846	30.380	3,344.069	30.062	0.435	29.570	30.554	1.64%
2	1,621.249	438,094.406	1,584.638	465,713.335	1,525.043	465,073.810	1,576.977	48.559	1,522.028	1,631.926	3.48%
3	1,586.039	463,508.552	1,527.275	454,804.587	1,587.890	425,334.637	1,567.068	34.474	1,528.056	1,606.079	2.49%
4	29.918	2,601.463	30.375	4,259.002	29.583	2,358.004	29.959	0.398	29.509	30.409	1.50%
5	1,544.600	434,520.236	1,568.070	422,970.240	1,496.546	431,185.570	1,536.405	36.459	1,495.148	1,577.662	2.69%
6	1,575.437	428,079.528	1,582.240	473,641.503	1,536.894	442,579.876	1,564.857	24.455	1,537.184	1,592.530	1.77%
7	288.654	177,941.538	342.113	173,185.099	277.840	155,929.313	302.869	34.414	263.926	341.812	12.86%
8	10,573.239	216,586.450	10,557.774	240,093.821	10,598.500	252,470.789	10,576.504	20.559	10,553.240	10,599.769	0.22%
9	9,859.367	260,823.001	9,946.041	254,981.754	9,922.443	247,450.757	9,909.284	44.810	9,858.576	9,959.991	0.51%
10	242.190	70,509.932	241.892	75,951.771	224.935	67,138.833	236.339	9.877	225.162	247.516	4.73%
11	3,096.918	651,817.336	3,053.348	680,232.106	3,117.611	647,971.318	3,089.293	32.803	3,052.173	3,126.413	1.20%
12	3,086.553	646,694.735	3,093.461	628,727.306	3,088.840	634,994.073	3,089.618	3.519	3,085.635	3,093.600	0.13%
13	264.394	71,383.632	249.562	72,544.505	267.306	84,281.321	260.420	9.516	249.652	271.189	4.14%
14	4,396.270	522,980.957	4,248.977	532,696.876	4,374.163	517,806.127	4,339.803	79.431	4,249.919	4,429.687	2.07%
15	4,328.760	551,533.456	4,324.125	539,825.399	4,303.086	561,568.342	4,318.657	13.683	4,303.173	4,334.140	0.36%
16	1,813.909	558,390.431	1,760.900	564,210.533	1,765.409	574,955.476	1,780.073	29.390	1,746.815	1,813.330	1.87%
17	13,373.582	150,870.878	13,384.273	164,856.569	13,419.556	146,060.772	13,392.470	24.059	13,365.246	13,419.695	0.20%
18	13,433.649	147,967.365	13,358.045	160,546.301	13,334.188	162,309.544	13,375.294	51.926	13,316.534	13,434.053	0.44%
19	730.973	168,857.569	724.492	162,469.721	728.079	171,839.960	727.848	3.247	724.174	731.522	0.50%
20	5,827.439	530,335.316	5,852.958	542,534.385	5,821.024	543,186.090	5,833.807	16.893	5,814.691	5,852.923	0.33%
21	5,655.496	587,041.156	5,546.214	553,193.885	5,654.601	537,596.241	5,618.771	62.837	5,547.664	5,689.877	1.27%
22	1,534.997	332,922.981	1,451.723	296,913.697	1,550.020	338,325.966	1,512.247	52.950	1,452.328	1,572.166	3.96%
23	10,592.753	241,010.124	10,601.366	244,240.078	10,731.927	243,510.305	10,642.015	77.985	10,553.767	10,730.264	0.83%
24	10,676.646	241,700.900	10,756.440	233,269.971	10,737.915	242,840.644	10,723.667	41.762	10,676.409	10,770.925	0.44%
25	2,852.620	372,916.706	3,019.244	408,213.136	2,773.291	404,657.327	2,881.718	125.532	2,739.665	3,023.771	4.93%
26	10,475.883	97,616.605	10,392.859	91,827.657	10,402.906	100,675.728	10,423.883	45.313	10,372.606	10,475.159	0.49%
27	10,387.467	93,187.330	10,424.332	92,106.978	10,481.954	97,270.783	10,431.251	47.622	10,377.362	10,485.140	0.52%
28	30.620	4,033.989	30.193	3,794.218	29.894	3,796.874	30.236	0.365	29.823	30.648	1.37%
29	1,573.371	265,252.300	1,599.206	257,623.602	1,605.636	265,773.803	1,592.738	17.077	1,573.413	1,612.063	1.21%
30	1,612.461	254,832.553	1,611.120	259,490.662	1,601.825	259,760.865	1,608.469	5.793	1,601.913	1,615.024	0.41%
31	76.151	19,859.760	75.567	22,857.806	75.343	22,299.653	75.687	0.417	75.214	76.159	0.62%
32	3,103.959	157,122.085	3,134.354	153,655.986	3,109.272	157,470.523	3,115.862	16.234	3,097.492	3,134.232	0.59%
33	3,122.420	153,501.464	3,132.908	152,015.002	3,137.998	162,013.921	3,131.109	7.943	3,122.120	3,140.097	0.29%
34	191.138	65,583.397	189.049	66,364.272	199.976	66,690.417	193.388	5.801	186.823	199.952	3.39%
35	2,003.026	7,926.237	2,003.109	7,931.114	2,009.625	7,497.891	2,005.253	3.786	2,000.969	2,009.538	0.21%
36	2,007.354	7,752.101	2,006.101	8,284.366	2,000.528	8,301.114	2,004.661	3.634	2,000.549	2,008.773	0.21%

S.D. = Standard Deviation

A.3 Clustered Network Data

Table A.8 Clustered Network Throughput ANOVA

Component	% Var	Deg.Free	F-Computed	F-Table
SST=	100	107		
Main Effects	73.9	7	201276.29	2.42
Size (S)	30.2	3	192128.53	3.01
Traffic (L)	28.3	2	269705.01	3.40
R_S **(C)**	15.4	2	146569.21	3.40
2nd-order Interactions	25.5	16	30391.81	2.09
SL	17.2	6	54789.83	2.51
SC	1.45	6	4619.72	2.51
LC	6.81	4	32452.92	2.78
3rd-order Interactions	0.561	12	891.71	2.18
Error	0.00126	24		

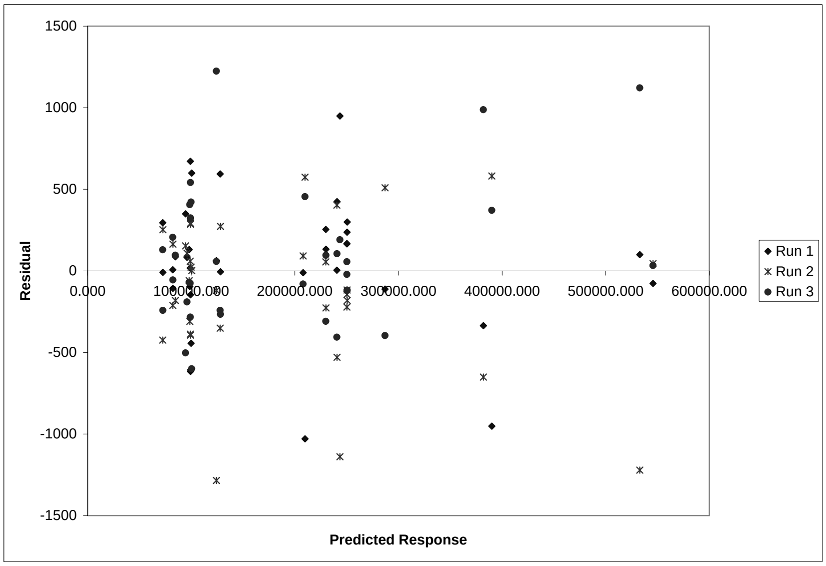


Figure A.3 Clustered Network Residual vs. Response Plot

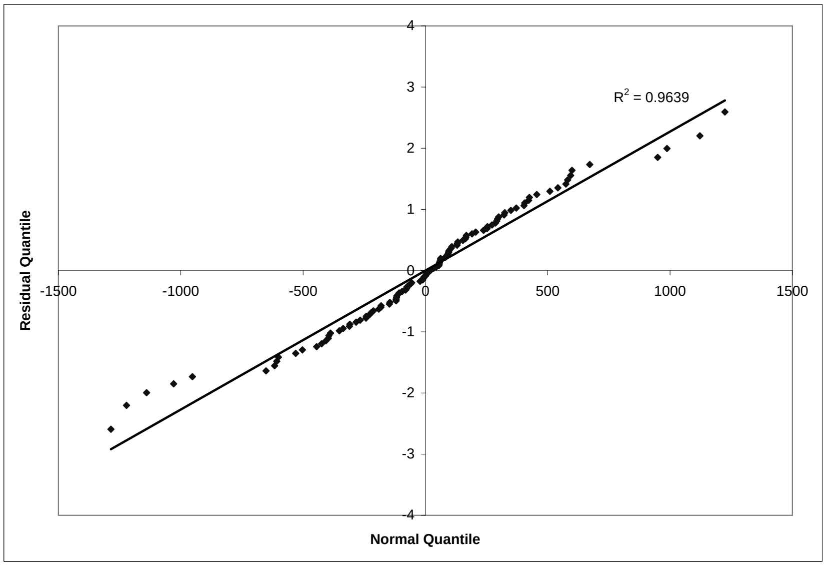


Figure A.4 Clustered Network Normal quantile-quantile Plot of Error

Table A.9 Clustered Network Simulation Results - Throughput (bits/sec)

Replication Run	1		2		3		Overall Mean	Overall S.D.	Lower 95% CI	Upper 95% CI	r
	Mean	S.D.	Mean	S.D.	Mean	S.D.					
1	101,018.23	9,753.56	100,420.71	9,920.63	99,818.53	9,704.61	100,419.16	599.86	99,740.36	101,097.96	0.68%
2	250,858.06	5,187.07	250,377.24	5,112.22	250,440.26	5,280.30	250,558.52	261.31	250,262.82	250,854.23	0.12%
3	250,428.59	5,418.56	250,041.14	5,226.26	250,318.89	5,485.64	250,262.87	199.71	250,036.88	250,488.87	0.09%
4	99,424.07	10,731.48	99,890.88	11,288.35	100,290.01	11,083.98	99,868.32	433.41	99,377.87	100,358.77	0.49%
5	250,615.32	5,506.19	250,260.54	5,471.83	250,258.21	5,390.57	250,378.02	205.51	250,145.47	250,610.58	0.09%
6	250,388.91	5,363.19	250,076.15	5,447.88	250,199.85	5,408.24	250,221.64	157.52	250,043.39	250,399.88	0.07%
7	98,695.84	10,063.65	99,589.79	10,426.53	99,624.80	10,204.92	99,303.48	526.52	98,707.67	99,899.29	0.60%
8	124,396.21	12,735.27	124,214.15	12,779.63	124,391.54	12,235.30	124,333.97	103.79	124,216.52	124,451.41	0.09%
9	124,361.20	12,983.74	123,014.44	12,523.57	125,523.56	11,389.95	124,299.73	1,255.69	122,878.79	125,720.68	1.14%
10	98,947.92	10,830.15	98,989.93	10,136.81	98,854.56	9,505.72	98,930.80	69.29	98,852.39	99,009.22	0.08%
11	241,036.32	6,337.44	240,081.69	7,129.27	240,716.56	7,106.92	240,611.52	485.91	240,061.67	241,161.38	0.23%
12	240,602.19	6,650.15	241,001.31	6,357.03	240,191.39	6,677.66	240,598.30	404.97	240,140.03	241,056.57	0.19%
13	98,460.10	10,212.94	98,245.37	10,258.74	98,961.93	10,128.56	98,555.80	367.74	98,139.66	98,971.93	0.42%
14	230,070.90	7,164.04	229,711.45	6,928.76	230,033.55	7,163.27	229,938.63	197.63	229,714.99	230,162.27	0.10%
15	230,094.24	7,326.92	229,895.84	7,027.68	229,531.73	7,137.12	229,840.60	285.29	229,517.76	230,163.44	0.14%
16	94,853.98	8,324.56	94,657.91	8,279.19	94,002.04	8,009.76	94,504.64	446.17	93,999.76	95,009.53	0.53%
17	82,168.34	6,833.74	82,439.10	6,837.20	82,219.69	6,756.54	82,275.71	143.81	82,112.98	82,438.44	0.20%
18	82,166.01	7,495.28	81,946.61	6,903.04	82,364.41	6,796.59	82,159.01	208.99	81,922.52	82,395.50	0.29%
19	98,074.98	10,075.26	97,883.59	9,970.74	97,874.25	9,729.09	97,944.27	113.29	97,816.07	98,072.48	0.13%
20	208,004.67	10,175.11	208,107.37	10,004.89	207,934.65	9,770.58	208,015.56	86.87	207,917.25	208,113.87	0.05%
21	208,793.58	10,449.13	210,397.08	10,028.02	210,278.05	10,409.48	209,822.90	893.40	208,811.92	210,833.88	0.48%
22	95,986.00	9,205.94	96,011.67	9,534.66	95,712.91	9,228.40	95,903.53	165.58	95,716.16	96,090.89	0.20%
23	128,172.72	12,871.15	128,450.47	12,172.48	127,911.31	12,723.24	128,178.17	269.63	127,873.06	128,483.28	0.24%
24	128,452.81	12,372.96	127,507.51	12,898.99	127,617.21	13,137.95	127,859.18	517.02	127,274.12	128,444.24	0.46%
25	84,752.15	7,927.52	84,483.73	7,813.83	84,761.49	7,989.33	84,665.79	157.73	84,487.30	84,844.29	0.21%
26	72,591.68	6,939.38	72,853.10	6,783.80	72,358.28	6,837.06	72,601.02	247.54	72,320.90	72,881.14	0.39%
27	72,771.41	6,463.47	72,052.52	6,634.15	72,605.69	6,937.81	72,476.54	376.45	72,050.55	72,902.53	0.59%
28	99,134.65	10,551.93	98,887.24	9,988.09	99,823.19	10,670.29	99,281.69	485.00	98,732.87	99,830.52	0.55%
29	389,158.28	18,827.76	390,691.76	18,370.16	390,481.69	16,821.36	390,110.58	831.38	389,169.79	391,051.37	0.24%
30	532,948.21	22,331.13	531,627.13	22,254.93	533,970.53	21,402.92	532,848.63	1,174.87	531,519.14	534,178.12	0.25%
31	98,684.17	9,759.57	99,592.12	10,068.40	99,624.80	10,283.83	99,300.36	533.89	98,696.21	99,904.52	0.61%
32	381,651.93	19,412.69	381,336.83	19,972.77	382,975.35	18,673.57	381,988.04	869.43	381,004.19	382,971.89	0.26%
33	545,568.49	23,274.59	545,689.86	22,877.07	545,678.19	22,530.71	545,645.51	66.96	545,569.74	545,721.29	0.01%
34	99,874.54	10,495.73	98,814.88	9,725.17	98,919.91	9,949.77	99,203.11	583.84	98,542.43	99,863.79	0.67%
35	244,430.05	17,697.08	242,341.06	17,618.54	243,671.48	17,635.88	243,480.87	1,057.46	242,284.24	244,677.49	0.49%
36	286,898.32	18,327.58	287,519.18	17,675.91	286,613.57	19,082.81	287,010.36	463.09	286,486.33	287,534.39	0.18%

S.D. = Standard Deviation

Table A.10 Clustered Network Simulation Results - Collisions (collisions/packet)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%	
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	r
1	0.000	0.000	0.002	0.047	0.000	0.000	0.001	0.001	0.000	0.002	196.000%
2	0.136	0.412	0.127	0.405	0.127	0.382	0.130	0.005	0.124	0.136	4.404%
3	0.112	0.361	0.140	0.432	0.125	0.386	0.125	0.014	0.109	0.142	12.842%
4	0.002	0.047	0.000	0.000	0.000	0.000	0.001	0.001	0.000	0.002	196.000%
5	0.140	0.416	0.166	0.452	0.162	0.487	0.156	0.014	0.140	0.172	10.199%
6	0.138	0.414	0.182	0.473	0.164	0.475	0.161	0.022	0.136	0.186	15.463%
7	0.118	0.355	0.131	0.369	0.116	0.347	0.122	0.008	0.112	0.131	7.696%
8	0.923	0.856	0.856	0.854	0.812	0.840	0.864	0.056	0.800	0.927	7.368%
9	0.838	0.864	0.860	0.829	0.766	0.764	0.821	0.049	0.766	0.877	6.784%
10	0.007	0.081	0.000	0.000	0.000	0.000	0.002	0.004	0.000	0.006	196.000%
11	0.123	0.372	0.116	0.377	0.116	0.359	0.118	0.004	0.114	0.122	3.630%
12	0.092	0.311	0.096	0.350	0.085	0.302	0.091	0.006	0.085	0.097	6.835%
13	0.024	0.153	0.028	0.179	0.035	0.184	0.029	0.006	0.023	0.035	21.359%
14	0.195	0.438	0.186	0.447	0.184	0.420	0.188	0.006	0.182	0.195	3.481%
15	0.212	0.469	0.201	0.458	0.177	0.426	0.197	0.018	0.177	0.217	10.292%
16	0.512	0.679	0.405	0.656	0.510	0.717	0.476	0.061	0.406	0.545	14.582%
17	1.639	0.915	1.523	0.946	1.584	0.933	1.582	0.058	1.516	1.648	4.150%
18	1.501	0.980	1.512	0.908	1.462	0.910	1.492	0.026	1.462	1.522	2.008%
19	0.015	0.123	0.013	0.114	0.007	0.081	0.012	0.005	0.007	0.017	44.168%
20	0.123	0.372	0.158	0.436	0.092	0.304	0.124	0.033	0.087	0.161	29.976%
21	0.105	0.321	0.118	0.368	0.109	0.319	0.111	0.007	0.103	0.118	6.823%
22	0.217	0.458	0.201	0.438	0.223	0.471	0.214	0.011	0.201	0.226	5.946%
23	0.792	0.810	0.818	0.851	0.842	0.823	0.818	0.025	0.789	0.846	3.484%
24	0.812	0.850	0.875	0.824	0.836	0.844	0.841	0.032	0.805	0.877	4.311%
25	0.764	0.859	0.709	0.773	0.810	0.817	0.761	0.050	0.704	0.818	7.496%
26	1.910	1.073	1.834	1.046	1.897	1.134	1.880	0.041	1.834	1.927	2.465%
27	1.915	1.129	1.853	1.046	1.781	1.126	1.850	0.067	1.774	1.925	4.087%
28	0.035	0.196	0.022	0.146	0.037	0.240	0.031	0.008	0.022	0.041	29.890%
29	0.416	0.630	0.374	0.654	0.400	0.645	0.397	0.021	0.373	0.421	5.996%
30	0.621	0.813	0.510	0.707	0.567	0.775	0.566	0.056	0.503	0.629	11.156%
31	0.061	0.258	0.072	0.267	0.085	0.316	0.073	0.012	0.059	0.087	18.697%
32	0.759	0.850	0.707	0.874	0.788	0.851	0.751	0.041	0.705	0.798	6.187%
33	0.950	0.932	0.954	1.007	0.965	1.015	0.956	0.008	0.947	0.965	0.934%
34	0.118	0.379	0.068	0.269	0.118	0.349	0.101	0.029	0.069	0.134	32.432%
35	1.004	0.989	1.123	1.042	1.000	1.045	1.042	0.070	0.964	1.121	7.547%
36	1.201	1.141	1.042	1.035	1.158	1.134	1.133	0.083	1.040	1.227	8.241%

S.D. = Standard Deviation

Table A.11 Clustered Network Simulation Results - Deferrals (slots/packet)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%		
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	+/-	r
1	30.127	2,505.087	29.852	2,591.233	29.575	2,344.408	29.852	0.276	29.540	30.164	0.312	1.05%
2	1,587.388	461,957.275	1,653.788	510,179.667	1,611.018	489,027.832	1,617.398	33.657	1,579.312	1,655.484	38.086	2.35%
3	1,604.963	448,133.721	1,659.985	450,705.791	1,639.738	453,425.827	1,634.895	27.829	1,603.404	1,666.387	31.492	1.93%
4	30.050	3,159.527	30.744	5,812.402	29.855	2,883.170	30.216	0.467	29.688	30.745	0.529	1.75%
5	1,650.789	484,463.436	1,593.279	448,247.326	1,610.920	470,860.565	1,618.329	29.462	1,584.990	1,651.669	33.339	2.06%
6	1,692.906	485,614.748	1,609.580	438,105.897	1,565.761	469,534.088	1,622.749	64.587	1,549.662	1,695.836	73.087	4.50%
7	176.941	89,967.757	185.508	115,147.322	176.360	89,233.659	179.603	5.122	173.807	185.399	5.796	3.23%
8	9,776.591	286,927.812	9,775.599	305,363.710	9,748.214	294,998.336	9,766.801	16.105	9,748.577	9,785.025	18.224	0.19%
9	9,763.837	280,562.932	9,877.390	293,341.815	9,674.558	297,179.354	9,771.928	101.658	9,656.892	9,886.965	115.037	1.18%
10	184.721	57,728.341	192.540	59,752.438	185.955	54,182.608	187.739	4.203	182.982	192.495	4.757	2.53%
11	2,942.969	618,908.369	2,940.954	593,413.080	2,902.055	611,590.721	2,928.659	23.062	2,902.562	2,954.757	26.097	0.89%
12	2,865.644	615,144.663	2,910.627	578,922.683	2,905.809	629,717.661	2,894.027	24.698	2,866.078	2,921.975	27.949	0.97%
13	225.665	65,281.300	217.445	66,730.044	219.790	68,339.907	220.967	4.235	216.175	225.759	4.792	2.17%
14	3,833.123	547,864.075	3,813.603	545,118.526	3,801.031	540,582.062	3,815.919	16.171	3,797.620	3,834.218	18.299	0.48%
15	3,823.876	546,796.191	3,859.564	560,017.792	3,849.957	571,412.818	3,844.466	18.467	3,823.569	3,865.363	20.897	0.54%
16	1,335.655	467,308.681	1,197.283	397,440.068	1,583.665	526,302.602	1,372.201	195.766	1,150.671	1,593.731	221.530	16.14%
17	13,313.265	174,131.605	13,250.657	166,889.505	13,304.422	173,589.282	13,289.448	33.883	13,251.105	13,327.791	38.343	0.29%
18	13,265.639	160,151.394	13,281.549	170,248.886	13,222.043	172,809.652	13,256.410	30.808	13,221.548	13,291.272	34.862	0.26%
19	451.486	117,131.857	454.996	109,949.858	479.721	122,319.389	462.068	15.389	444.654	479.482	17.414	3.77%
20	4,104.749	558,930.808	4,075.268	544,714.705	4,152.848	535,571.348	4,110.955	39.160	4,066.641	4,155.269	44.314	1.08%
21	4,151.322	534,224.737	4,182.875	535,379.188	4,180.029	613,297.406	4,171.408	17.454	4,151.658	4,191.159	19.751	0.47%
22	798.504	183,853.827	845.316	193,440.671	866.877	199,866.079	836.899	34.955	797.343	876.454	39.556	4.73%
23	9,037.693	300,591.583	9,010.403	293,179.498	8,966.664	286,306.998	9,004.920	35.831	8,964.374	9,045.467	40.546	0.45%
24	8,995.802	295,686.263	9,044.008	283,799.190	9,109.067	281,771.208	9,049.625	56.841	8,985.304	9,113.947	64.322	0.71%
25	2,885.092	556,011.714	3,086.707	562,211.648	3,045.665	527,618.295	3,005.821	106.549	2,885.249	3,126.393	120.572	4.01%
26	13,802.139	124,600.900	13,748.289	132,453.943	13,800.928	129,284.158	13,783.785	30.747	13,748.992	13,818.579	34.794	0.25%
27	13,708.334	136,124.149	13,879.280	133,953.730	13,750.815	137,945.320	13,779.477	89.004	13,678.759	13,880.194	100.718	0.73%
28	115.944	32,811.404	115.989	33,232.036	108.783	28,346.857	113.572	4.147	108.879	118.266	4.693	4.13%
29	835.337	198,514.939	830.782	203,260.391	835.240	206,065.366	833.787	2.602	830.842	836.731	2.945	0.35%
30	644.706	216,170.063	642.311	222,981.319	651.015	214,064.581	646.011	4.496	640.923	651.099	5.088	0.79%
31	139.304	41,336.069	134.996	35,311.363	138.947	39,865.856	137.749	2.391	135.044	140.455	2.705	1.96%
32	1,166.523	179,501.434	1,171.070	183,900.644	1,168.490	181,707.452	1,168.694	2.280	1,166.114	1,171.274	2.580	0.22%
33	957.463	194,068.878	955.079	182,334.469	958.615	187,061.069	957.052	1.803	955.011	959.093	2.041	0.21%
34	219.356	75,605.453	214.092	75,469.993	204.645	67,837.666	212.698	7.454	204.263	221.133	8.435	3.97%
35	2,790.344	96,576.719	2,817.799	102,538.847	2,807.667	100,183.615	2,805.270	13.884	2,789.559	2,820.981	15.711	0.56%
36	2,412.686	112,245.405	2,410.383	104,302.192	2,426.619	100,237.338	2,416.563	8.785	2,406.622	2,426.504	9.941	0.41%

S.D. = Standard Deviation

A.4 5-Node Network Data

Table A.12 5-Node Network Throughput ANOVA

Component	**% Var**	**Deg.Free**	**F-Computed**	**F-Table**
SST=	100	107		
Main Effects	82.8	7	196132.14	2.42
Size (S)	9.92	3	54770.54	3.01
Traffic (L)	25.4	2	210834.76	3.40
R_S **(C)**	47.5	2	393471.92	3.40
2nd-order Interactions	14.4	16	14940.81	2.09
SL	2.21	6	6096.96	2.51
SC	5.02	6	13857.41	2.51
LC	7.20	4	29831.70	2.78
3rd-order Interactions	0.03	12	3760.36	2.18
Error	0.00145	24		

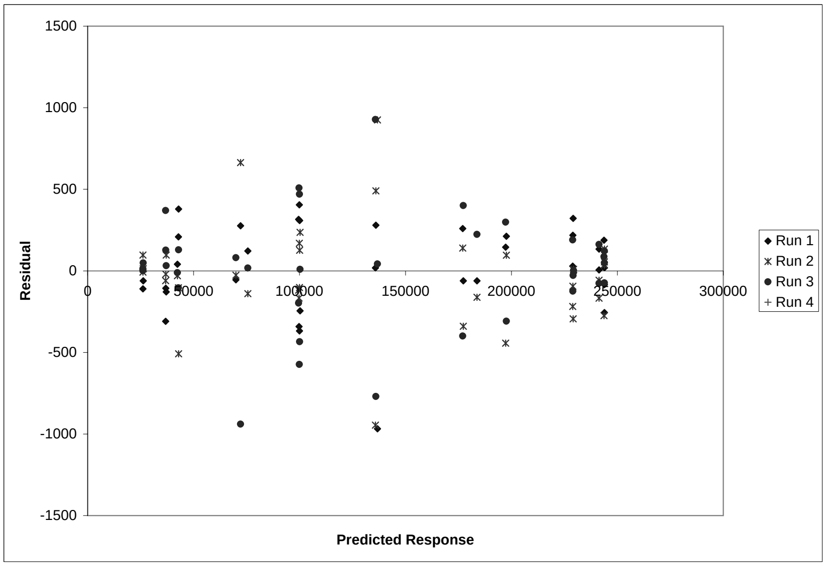


Figure A.5 5-Node Network Residual vs. Response Plot

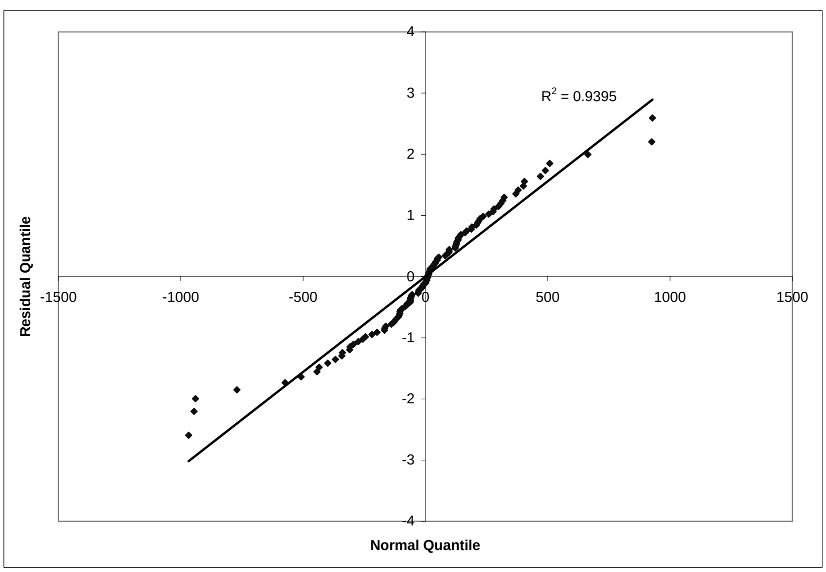


Figure A.6 5-Node Network Normal quantile-quantile Plot of Error

Table A.13 5-Node Network Simulation Results - Throughput (bits/sec)

Replication Run	1 Mean	1 S.D.	2 Mean	2 S.D.	3 Mean	3 S.D.	Overall Mean	Overall S.D.	Lower 95% CI	Upper 95% CI	r
1	100,308.680	10,064.809	100,072.939	10,896.234	99,330.708	10,132.735	99,904.109	510.378	99,326.562	100,481.656	0.58%
2	243,676.149	4,023.769	244,065.937	4,251.968	244,054.267	3,993.876	243,932.118	221.752	243,681.181	244,183.054	0.10%
3	243,893.217	3,787.735	243,431.072	3,786.276	243,792.852	4,096.254	243,705.714	243.083	243,430.640	243,980.788	0.11%
4	100,371.699	10,326.575	100,189.643	9,786.699	99,629.468	10,524.896	100,063.603	386.835	99,625.858	100,501.349	0.44%
5	243,895.551	4,072.690	243,930.562	3,762.170	243,802.188	3,969.897	243,876.100	66.360	243,801.007	243,951.194	0.03%
6	243,809.190	4,123.305	243,928.228	3,907.386	243,942.232	4,166.881	243,893.217	73.105	243,810.491	243,975.943	0.03%
7	69,884.172	11,436.122	69,912.181	10,627.462	70,019.548	11,166.629	69,938.634	71.459	69,857.770	70,019.498	0.12%
8	135,828.446	11,581.196	137,721.371	12,474.225	136,839.096	11,678.495	136,796.304	947.188	135,724.461	137,868.148	0.78%
9	183,669.730	5,266.585	183,569.365	4,941.833	183,954.486	5,466.734	183,731.194	199.782	183,505.119	183,957.268	0.12%
10	99,620.131	10,679.186	99,886.214	9,823.374	100,458.060	9,907.648	99,988.135	428.161	99,503.625	100,472.645	0.48%
11	241,344.420	4,292.324	241,171.699	4,231.601	241,500.802	4,338.086	241,338.974	164.619	241,152.690	241,525.258	0.08%
12	241,475.128	4,634.977	241,283.735	4,687.991	241,265.062	4,247.674	241,341.308	116.267	241,209.740	241,472.876	0.05%
13	99,858.206	10,509.721	99,424.070	10,159.134	99,344.712	10,562.720	99,542.329	276.420	99,229.531	99,855.128	0.31%
14	229,225.966	5,444.770	228,913.202	5,418.064	228,882.859	4,905.785	229,007.343	189.941	228,792.404	229,222.281	0.09%
15	229,480.379	5,191.161	228,864.187	5,198.433	229,130.270	5,090.235	229,158.279	309.050	228,808.556	229,508.001	0.15%
16	42,435.594	6,468.552	42,365.573	6,542.390	42,384.245	6,309.885	42,395.137	36.259	42,354.106	42,436.169	0.10%
17	43,035.449	6,821.477	42,722.684	6,382.186	42,722.684	6,311.817	42,826.939	180.575	42,622.600	43,031.278	0.48%
18	43,299.198	6,654.266	42,412.254	6,510.738	43,049.453	6,142.002	42,920.301	457.359	42,402.751	43,437.852	1.21%
19	100,021.590	10,128.269	100,502.407	10,797.638	100,276.003	9,760.576	100,266.667	240.544	99,994.465	100,538.868	0.27%
20	229,319.329	5,106.259	229,340.336	5,193.243	229,333.333	4,988.626	229,330.999	10.696	229,318.896	229,343.103	0.01%
21	228,931.875	5,064.392	228,684.464	5,423.539	229,092.925	5,209.267	228,903.088	205.746	228,670.264	229,135.912	0.10%
22	72,411.962	10,703.572	72,799.416	11,869.866	71,195.915	10,912.095	72,135.765	836.671	71,188.983	73,082.547	1.31%
23	136,327.936	12,634.313	136,538.001	13,251.114	135,277.608	12,576.870	136,047.848	675.267	135,283.712	136,811.984	0.56%
24	135,844.785	12,735.958	134,880.817	12,942.206	136,755.069	12,213.998	135,826.890	937.254	134,766.287	136,887.493	0.78%
25	36,959.883	4,680.509	37,186.287	4,787.069	37,120.934	4,671.678	37,089.035	116.524	36,957.175	37,220.894	0.36%
26	36,525.748	4,471.694	36,775.492	4,622.045	37,204.960	4,673.680	36,835.400	343.546	36,446.641	37,224.159	1.06%
27	36,775.492	4,847.075	36,861.853	4,758.420	37,008.899	4,774.127	36,882.081	118.011	36,748.540	37,015.623	0.36%
28	99,463.749	10,813.845	99,638.804	10,535.884	100,313.348	10,509.144	99,805.300	448.604	99,297.657	100,312.943	0.51%
29	197,419.694	10,240.371	196,831.510	9,931.364	197,573.742	10,171.892	197,274.982	391.706	196,831.725	197,718.238	0.22%
30	197,839.825	10,267.376	197,723.122	10,000.480	197,319.329	9,569.793	197,627.425	273.125	197,318.355	197,936.496	0.16%
31	75,712.327	8,052.355	75,450.912	8,876.852	75,607.294	9,024.963	75,590.177	131.545	75,441.320	75,739.035	0.20%
32	177,295.405	8,796.382	177,176.368	8,927.192	176,637.199	8,962.862	177,036.324	350.739	176,639.425	177,433.222	0.22%
33	177,216.047	9,559.504	176,938.293	9,386.632	177,678.191	9,068.289	177,277.510	373.759	176,854.563	177,700.458	0.24%
34	26,013.129	2,324.986	26,220.861	2,406.579	26,136.834	2,391.535	26,123.608	104.495	26,005.360	26,241.856	0.45%
35	26,129.832	2,388.403	26,115.828	2,355.733	26,125.164	2,309.792	26,123.608	7.131	26,115.539	26,131.677	0.03%
36	26,174.179	2,358.619	26,248.869	2,436.314	26,283.880	2,284.223	26,235.643	56.034	26,172.235	26,299.051	0.24%

S.D. = Standard Deviation

Table A.14 5-Node Network Simulation Results - Collisions (collisions/packet)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%	
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	r
1	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	-
2	0.039	0.216	0.033	0.201	0.059	0.279	0.044	0.014	0.028	0.059	35.334%
3	0.050	0.229	0.050	0.229	0.035	0.184	0.045	0.009	0.035	0.055	22.129%
4	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	-
5	0.042	0.200	0.031	0.217	0.061	0.249	0.044	0.016	0.027	0.062	39.483%
6	0.042	0.211	0.033	0.178	0.033	0.190	0.036	0.005	0.030	0.041	16.000%
7	0.044	0.205	0.033	0.178	0.042	0.200	0.039	0.006	0.033	0.046	16.633%
8	0.044	0.205	0.039	0.195	0.039	0.195	0.041	0.003	0.038	0.044	7.000%
9	0.037	0.211	0.031	0.173	0.028	0.166	0.032	0.005	0.027	0.037	16.061%
10	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	-
11	0.042	0.211	0.039	0.195	0.042	0.221	0.041	0.001	0.039	0.042	3.500%
12	0.053	0.251	0.057	0.250	0.037	0.189	0.049	0.010	0.037	0.061	23.945%
13	0.009	0.093	0.015	0.123	0.013	0.114	0.012	0.003	0.009	0.016	30.504%
14	0.063	0.261	0.070	0.255	0.066	0.257	0.066	0.003	0.063	0.070	5.699%
15	0.048	0.224	0.044	0.205	0.077	0.282	0.056	0.018	0.036	0.076	35.908%
16	0.151	0.364	0.158	0.365	0.177	0.388	0.162	0.014	0.146	0.177	9.550%
17	0.118	0.323	0.151	0.364	0.186	0.395	0.152	0.034	0.113	0.190	25.302%
18	0.162	0.375	0.158	0.382	0.142	0.350	0.154	0.010	0.142	0.166	7.603%
19	0.011	0.104	0.009	0.093	0.015	0.123	0.012	0.003	0.008	0.015	32.410%
20	0.098	0.298	0.077	0.266	0.072	0.259	0.082	0.014	0.067	0.098	19.315%
21	0.092	0.289	0.077	0.290	0.077	0.266	0.082	0.009	0.072	0.092	12.250%
22	0.116	0.321	0.090	0.286	0.116	0.321	0.107	0.015	0.090	0.124	16.000%
23	0.160	0.379	0.175	0.392	0.177	0.382	0.171	0.010	0.160	0.181	6.324%
24	0.162	0.375	0.138	0.345	0.184	0.388	0.161	0.023	0.135	0.187	16.135%
25	0.219	0.440	0.239	0.461	0.214	0.437	0.224	0.013	0.209	0.238	6.479%
26	0.179	0.422	0.217	0.458	0.212	0.425	0.203	0.020	0.180	0.226	11.346%
27	0.210	0.429	0.210	0.429	0.193	0.432	0.204	0.010	0.193	0.216	5.600%
28	0.020	0.139	0.007	0.081	0.013	0.114	0.013	0.007	0.006	0.021	56.580%
29	0.061	0.240	0.096	0.295	0.092	0.289	0.083	0.019	0.062	0.105	25.961%
30	0.070	0.255	0.066	0.248	0.085	0.280	0.074	0.010	0.062	0.085	15.884%
31	0.024	0.153	0.028	0.166	0.022	0.146	0.025	0.003	0.021	0.029	15.252%
32	0.079	0.270	0.109	0.319	0.094	0.292	0.094	0.015	0.077	0.111	18.422%
33	0.096	0.295	0.092	0.289	0.088	0.283	0.092	0.004	0.087	0.097	5.389%
34	0.053	0.223	0.042	0.200	0.031	0.185	0.042	0.011	0.029	0.054	29.779%
35	0.042	0.200	0.042	0.200	0.039	0.195	0.041	0.001	0.039	0.042	3.500%
36	0.044	0.205	0.053	0.223	0.042	0.200	0.046	0.006	0.039	0.053	14.257%

S.D. = Standard Deviation

Table A.15 5-Node Network Simulation Results - Deferrals (slots/packet)

Replication	1		2		3		Overall	Overall	Lower 95%	Upper 95%	
Run	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	CI	CI	r
1	26.466	1,976.688	26.476	1,934.743	26.307	1,914.407	26.417	0.095	26.309	26.524	0.41%
2	93.747	22,267.110	94.202	20,969.337	94.655	26,250.405	94.201	0.454	93.688	94.715	0.55%
3	94.306	22,201.527	93.931	22,553.985	93.018	13,657.214	93.752	0.663	93.002	94.501	0.80%
4	26.562	1,990.383	26.212	1,779.077	26.486	1,987.510	26.420	0.184	26.212	26.628	0.79%
5	92.746	19,815.125	91.448	10,192.430	94.596	23,632.807	92.930	1.582	91.140	94.720	1.93%
6	95.326	29,845.786	93.290	18,986.667	93.305	22,336.079	93.974	1.171	92.649	95.299	1.41%
7	1,743.503	41,262.932	1,732.691	45,152.958	1,717.871	43,569.100	1,731.355	12.868	1,716.793	1,745.917	0.84%
8	1,278.999	69,311.738	1,260.077	69,255.264	1,271.181	67,248.189	1,270.086	9.508	1,259.326	1,280.845	0.85%
9	1,173.418	100,309.153	1,174.555	101,438.706	1,172.063	98,763.595	1,173.345	1.247	1,171.934	1,174.757	0.12%
10	26.491	1,921.401	26.762	2,044.670	26.640	1,861.159	26.631	0.136	26.478	26.785	0.58%
11	94.527	32,784.141	93.293	21,866.715	92.441	19,560.776	93.421	1.049	92.234	94.607	1.27%
12	92.566	22,793.122	91.302	23,966.107	91.251	14,126.046	91.707	0.745	90.863	92.550	0.92%
13	51.713	16,396.778	50.618	15,013.731	52.984	16,295.651	51.772	1.184	50.431	53.112	2.59%
14	331.196	62,700.306	330.541	64,994.999	332.084	61,473.535	331.274	0.774	330.398	332.150	0.26%
15	331.466	67,511.156	336.934	63,427.898	327.858	63,719.602	332.086	4.569	326.915	337.257	1.56%
16	2,975.055	31,704.155	2,988.633	33,108.131	2,997.171	32,085.105	2,986.953	11.154	2,974.331	2,999.574	0.42%
17	2,960.382	33,614.555	2,975.492	32,501.042	2,973.121	31,624.918	2,969.665	8.126	2,960.470	2,978.861	0.31%
18	2,932.518	34,869.804	2,997.994	33,383.415	2,936.632	33,467.307	2,955.715	36.673	2,914.215	2,997.214	1.40%
19	30.802	4,219.326	30.996	3,952.486	31.105	3,785.961	30.968	0.154	30.794	31.142	0.56%
20	263.961	61,949.314	260.522	63,022.386	262.381	63,028.068	262.288	1.721	260.340	264.236	0.74%
21	257.706	61,770.626	259.138	62,832.113	260.881	59,233.474	259.242	1.590	257.442	261.041	0.69%
22	1,603.884	43,447.660	1,600.095	42,969.172	1,626.264	43,900.454	1,610.081	14.143	1,594.077	1,626.085	0.99%
23	1,154.052	63,719.980	1,146.700	67,007.066	1,163.739	71,105.112	1,154.830	8.546	1,145.159	1,164.501	0.84%
24	1,163.540	64,106.135	1,161.361	63,474.138	1,149.619	64,800.481	1,158.173	7.488	1,149.700	1,166.647	0.73%
25	2,043.329	17,262.502	2,024.847	18,084.565	2,027.217	17,014.043	2,031.798	10.057	2,020.418	2,043.178	0.56%
26	2,068.296	17,655.000	2,050.367	17,058.253	2,028.439	16,541.451	2,049.034	19.962	2,026.445	2,071.623	1.10%
27	2,049.156	17,063.812	2,051.846	16,772.509	2,031.879	17,130.079	2,044.294	10.836	2,032.032	2,056.555	0.60%
28	42.852	8,115.326	42.686	7,710.981	42.109	7,714.773	42.549	0.390	42.108	42.990	1.04%
29	453.702	56,718.066	451.383	54,345.816	451.000	55,384.172	452.028	1.462	450.374	453.683	0.37%
30	453.642	55,180.199	444.859	56,021.525	451.818	54,065.604	450.106	4.635	444.861	455.351	1.17%
31	450.779	15,426.609	447.469	15,426.047	449.681	13,968.377	449.310	1.686	447.402	451.217	0.42%
32	566.964	45,076.045	564.956	48,117.433	562.894	49,446.078	564.938	2.035	562.636	567.240	0.41%
33	570.568	51,299.333	558.662	47,172.512	560.437	46,524.070	563.222	6.423	555.954	570.490	1.29%
34	2,150.931	3,011.165	2,131.794	3,491.885	2,139.829	3,490.348	2,140.851	9.609	2,129.977	2,151.725	0.51%
35	2,140.351	3,271.949	2,141.468	3,274.194	2,140.612	3,131.088	2,140.810	0.584	2,140.150	2,141.471	0.03%
36	2,136.686	3,323.421	2,129.637	3,188.464	2,125.295	3,128.036	2,130.539	5.749	2,124.034	2,137.044	0.31%

S.D. = Standard Deviation

Appendix B. OPNET Simulator

This appendix contains an overview of the Optimum Performance NETwork Modeler (OPNET). It describes the default radio transceiver pipeline stages OPNET provides and the shortcomings of the simulator when applied to ad-hoc networks. Finally, the chapter presents how the default model was modified to correct for these shortcomings.

B.1 OPNET Overview

OPNET is a powerful discrete event network simulation tool. It allows designers to combine independently authored components into a custom network. Network design is broken into three general domains.

- Network Domain - This high level domain describes how nodes are interconnected and physically related to one another. There is only one network domain per simulation.
- Node Domain - Nodes can represent a variety of objects such as workstations, routers, satellites or servers. This domain describes a node and how it handles sent and received information. The operation of the node is determined by the node model. Node models consist of interacting modules of three varieties: processor modules, queue modules and communication modules. Processor modules execute general code and thus may perform a wide variety of functions. Queue modules serve to organize data. Communication modules transmit and receive data across communication links.
- Process Domain - This low level domain consist of the programming code used to manipulate data and collect statistics.

B.2 Radio Link Transceiver Pipeline

OPNET provides three types of communication links: point-to-point, bus, and radio. The simulation of a packet transmission across a link is accomplished through the use of a transceiver pipeline. The transceiver pipeline consist of stages that model different aspects of the link. The sequence of the stages and their interface are standardized for each link. However, the pipeline procedure executed in each stage is user supplied. In practice, this allows a user to select the communications protocol used across the link.

The Radio Link Transceiver Pipeline is illustrated in Figure B.1. It consist of fourteen stages. Stages 0 through 8 are executed at the time of packet transmission while stages 9 through 13 are executed at the time of packet reception. A description of each stage is given below and is based on the descriptions provided by Rapallo [Rap02].

Receiver Group - Stage 0 This stage is invoked only once per pair of transmitter and receiver channels. For each transmitter, this stage determines which channels can feasibly receive a transmission.

Transmission Delay - Stage 1 This stage is used to compute the transmission delay of a specific packet. Since this value is identical for all receivers, it is only executed once per transmission. After this stage, the packet is duplicated for each receiver and each subsequent pipeline stage is execute for each duplicated packet.

Link Closure - Stage 2 This stage determines whether communication between a transmitter and receiver is possible on a dynamic basis. If this stage determines that a transmission is not possible, the packet is destroyed.

Channel Match - Stage 3 This stage compares properties of the transmitting and receiving channel. Such properties include frequency, data rate, modulation

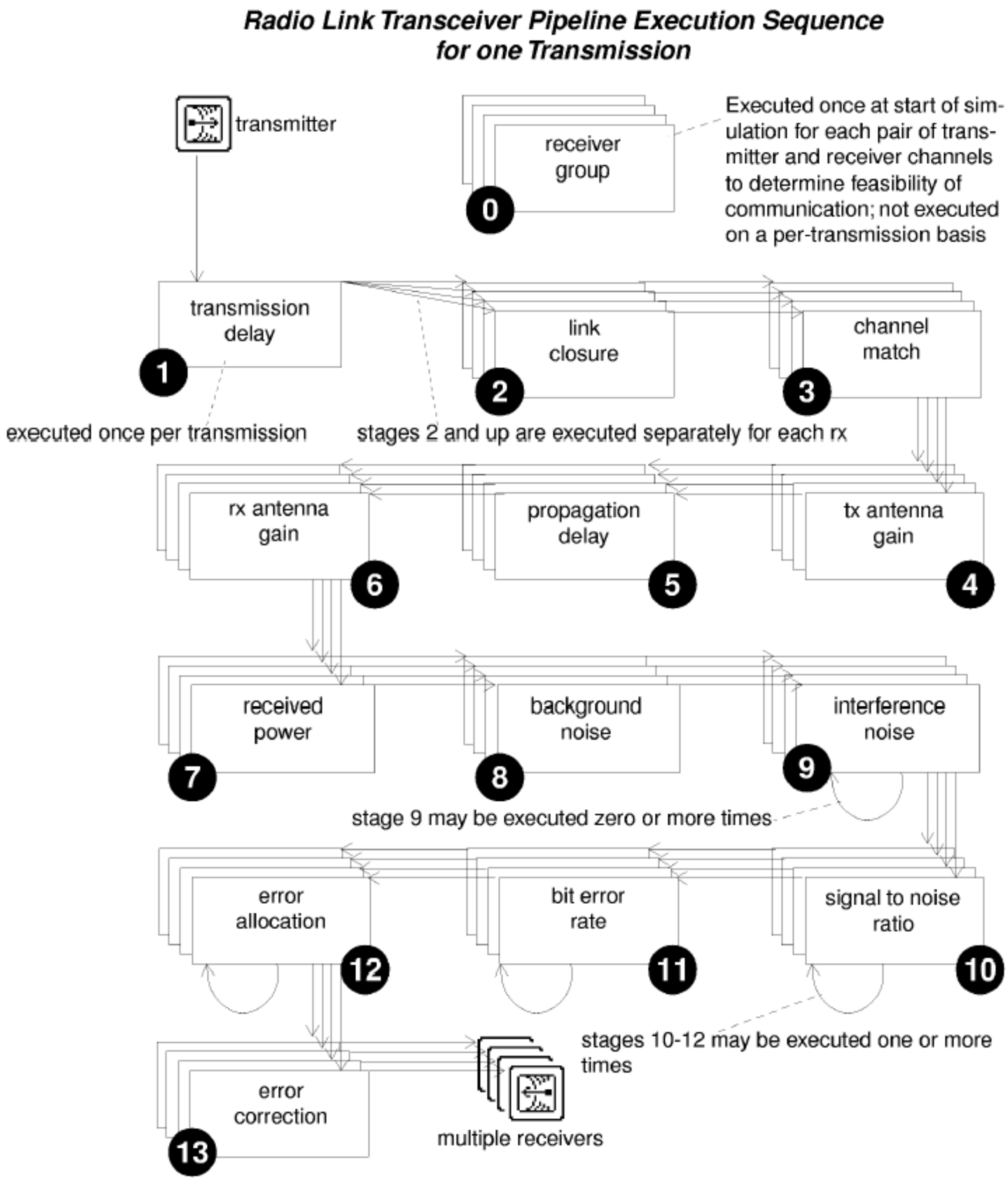


Figure B.1 Radio Link Transceiver Pipeline Execution Sequence for One Transmission [OPN01]

and spreading code. Depending on the results of the calculation, the packet match attribute is set to valid, noise or ignore.

TX Antenna Gain - Stage 4 This stage takes the receiving antenna characteristics and antenna position to compute the antenna gain. Since this study did not use antennas, a gain of one is always produced.

Propagation Delay - Stage 5 This stage computes the distance between the transmitting and receiving antennas and then calculates the propagation delay depending on the medium.

RX Antenna Gain - Stage 6 This stage is similar to Stage 4 and computes the receiver antenna gain. Since this study did not use antennas, a gain of one is always produced.

Received Power - Stage 7 This stage computes the received signal power taking into consideration the antenna gains and signal attenuation.

Background Noise - Stage 8 This stage computes the white gaussian noise present in the transmission medium and then sets the noise attribute of the packet.

Interference Noise - Stage 9 This stage computes noise created by interfering packets during propagation. If the interfering packet's channel match attribute is set to valid or noise then its power will be added to the packet of interest. The noise level of the interfering packet is adjusted as well. Whichever packet began reception first is deemed the *previous* packet. The packet beginning reception during reception of a *previous* packet is deemed the *arriving* packet. One or both of the packets must be valid for this stage to occur. This stage can be repeated zero or more times depending on the number of interfering packets. It occurs at the time of reception for the *previous* packet. When the interference stage is called, the packet is effectively broken into packet segments in which separate SNRs and BERs are calculated.

Signal-to-Noise Ratio - Stage 10 This stage computes the SNR for each packet segment and is repeated one or more times depending on the number of interferers. It is combined with the bit-error-rate stage and the error-allocation in an iteration set. The iteration must complete before any stage repeats. The SNR stage divides the received power by the noise calculated in the interference noise stage. This stage occurs after all the interference stages have been completed and the packet is fully segmented. The OPNET kernel adjusts the noise level for each segment and each repetition of the SNR stage.

Bit Error Rate - Stage 11 The BER is computed here for the packet segment. The segment length is defined by subtracting the current simulation time by the last SNR calculation time and then multiplying by the data rate.

Error Allocation - Stage 12 This stage uses the BER calculated in stage 11 and increments the packet's bit error counter using probabilistic methods.

Error Correction - Stage 13 This stage compares the number of bit errors to a designated threshold and decides whether the packet is accepted or rejected.

B.3 Modifications to Default WLAN Model

OPNET's WLAN process model implements the IEEE 802.11 MAC protocol. However, the WLAN model assumes a fully connected wireless network with a maximum span of 300 meters. These assumptions lead to several deficiencies in the model. First, all nodes detect a transmission regardless of the range and transmission power of the source. In fact, transmission power is neglected by the model. Successful reception is based entirely on whether the nodes are within 300 feet of each other. SNR is not utilized to determine the result of a transmission and interference between packets does not occur. These deficiencies render the model insufficient for simulating ad-hoc networks.

The MITRE Corporation developed an OPNET model implementing the MobileMesh ad-hoc routing protocol [GS]. A routing protocol discovers routes and

directs packets along those routes within an ad-hoc network. In order to implement MobileMesh, changes were made to the default WLAN MAC protocol and default pipeline stages. These changes correct the deficiencies of the default model. For this study, the changes made to the MAC layer and pipeline stages were utilized, however the routing protocol was not used.

B.4 Study Specific Modifications

The MobileMesh code was further modified to allow for this study. These changes are summarized below.

Received Power The MobileMesh code modified the received power pipeline stage so that the sig_lock attribute depends on the SNR of the received packet. The sig_lock attribute signifies that the channel has locked onto the current packet. If, while receiving the current packet, another packet arrives at the receiver, the later packet is characterized as noise even if it has a higher SNR value. This study modified the code such that the SNR threshold at which signal lock is triggered is coordinated with the CCA threshold.

In particular, if the CCA threshold is P_{cca}, then the SNR threshold is set according to:

$$SNR_{threshold} = G_{Proc} + 10 log \left(\frac{P_{cca}}{N_a} \right) \tag{B.1}$$

where G_{Proc}, processing gain, equals 10.41 and N_a, ambiant background noise, equals $4.0412E - 13$. If the SNR of a received packet ($SNR_{received}$) is such that $SNR_{received} > SNR_{threshold}$, then the sig_lock attribute is set to true.

Receiver Stat Wire The receiver module within the node model communicates to the MAC process through a stat wire. This stat wire interrupts the MAC model to inform it of an incoming packet. However, this wire creates an interrupt only if the incoming packet has an SNR greater than the wire's High

Threshold Trigger. This trigger value is set to the desired CCA threshold value. Previously, this trigger value was statically set. The model was modified to allow modification of the value for each run.

Target Selection Each node transmits to all other nodes randomly or to one specific node as specified by the user. Transmission to a specific node is useful for validation and debugging purposes. When transmitting to all nodes, a node address is uniformly randomly selected among all possible addresses. To approximate the added efficiency of a routing protocol, a target is randomly selected until one is chosen that is within 300 meters of the transmitting node.

Statistic Collection Code was added to allow collection of packet collision and node deferral statistics.

Bug Correction A bug was identified in the MobileMesh code that caused the model to attempt transmission of a zero sized data packet. According to IEEE 802.11, whenever a bad data packet is received, a collision is assumed and the node must backoff. This can occur even if the node does not have data to transmit. However, when the model leaves the Backoff state, it assumes that it must have data to transmit and transitions to the Transmit state. This bug was corrected by modifying the state transition conditions such that a transition to the Transmit state only occurs if a packet needs to be sent, otherwise the model transitions to the Idle state.

B.5 Model Validation

Validation of this model was conducted in two phases. The first was a process of code examination. Within OPNET's debugger, the model continually displays its current status. Using this feature, the model behaviour was inspected to ensure it properly responded to events.

Once the model was assured to behave logically correct, its output statistics were compared against expected values. This was to ensure the sensing range at-

tribute was behaving as expected. To accomplish this, a four-node network was constructed. The hidden and exposed node scenarios as depicted in Figures B.2 and B.3 were constructed with each node 250 meters apart. These scenarios are explained in Section 2.4.1. Each scenario was simulated using a packet load of 256,000 bps per node.

The results of these tests are shown in Tables B.1 and B.2. These results show that as the sensing range is decreased the number of collisions increase. However, even with an increase in collisions, throughput also rises. This generally coincides with expected performance. Both networks performed very similar to each other which is also generally expected since the receiving nodes must transmit ACK signals. This introduces two-way traffic into both scenarios leading us to expect the sensing range to affect both similarly.

Table B.1 Validation Exposed Node Scenario

	Throughput (bits/sec)	**Collisions (coll./pkt.)**	**Deferrals (slots/sec)**
$2R_c$	230011	0	16.911
$1R_c$	230011.73	0	16.911
$.5R_c$	297335.467	0.12	21.77

The number of deferrals also increases as the sensing range is decreased. Although we expected that the number of unnecessary deferrals should actually decrease, it must be remembered that the deferral statistic considers all deferrals, not just unecessary ones. We decided not to implement a deferral statistic that con-

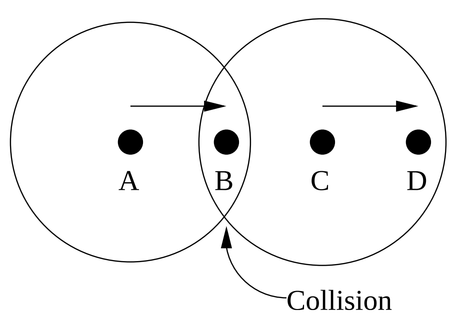


Figure B.2 Hidden Node Scenario

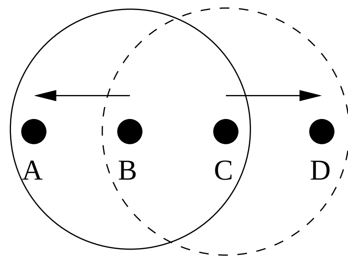


Figure B.3 Exposed Node Scenario

Table B.2 Validation Hidden Node Scenario

Sensing Range	**Throughput (bits/sec)**	**Collisions (coll./pkt.)**	**Deferrals (slots/sec)**
$2R_c$	224172.8	0.052	37.84
$1R_c$	224172.8	0.052	37.84
$.5R_c$	228213.33	0.076	38.97

sidered only unnecessary deferrals as this would have greatly increased the model overhead and would not have significantly contributed to the main focus of this study.

Bibliography

[Abr70] Abramson, Norman. "The ALOHA system - Another Alternative for Computer Communications." *1970 Fall Joint Computing Conference, AFIPS Conference Proceedings*, Vol. 37, pp. 281–285. Montvale, NJ: AFIPS Press, 1970.

[Abr77] Abramson, Norman. "The Throughput of Packet Broadcasting Channels." *IEEE Transaction in Communications*, Vol. COM-25, pp. 117–128. 1977.

[BDSZ94] Bharghavan, Vaduvur, Alan Demers, Scott Shenker, and Lixia Zhang. "MACAW: A Media Access Protocol for Wireless LAN's." *Proceedings of SIGCOMM '94 Conference.*, pp. 212–225. New York, NY: ACM Press, 1994. SIGCOMM is an ACM Special Interest Group on Data Communication.

[CH75] Carleial, Aydano B. and Martin E. Hellman. "Bistable Behavior of ALOHA-Type Systems." *IEEE Transactions in Communications*, COM-23(4):401–410, April 1975.

[FGB96] Fu, K., Y.J. Guo, and S.K. Barton. "Performance of the EY-NPMA Protocol." *Wireless Personal Communications*, 4:41–50, 1996.

[GL00] Gumalla, Ajay Chandra V. and John O. Limb. "Wireless Collision Detect (WCD): Multiple Access with Receiver Initiated Feedback and Carrier Detect Signal." *IEEE International Conference on Communications. ICC 2000. Global Convergence Through Communications. Conference Record*, pp. 397–401. Piscataway, NJ: IEEE, 2000.

[GS] Grace, Kevin H. and John A. Stine. "OPNET 7.0.B Simulation Model." The MITRE Corporation. Code and documentation available at www.opnet.com.

[HT99] Haas, Zygmunt J. and Siamak Tabrizi. "Collision-Free Medium Access Control Scheme for Ad-Hoc Networks." *IEEE Proceedings of Conference on Military Communications (MILCOM'99)*, pp. 276–280. Piscataway, NJ, 1999.

[IEE99] IEEE. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." *ANSI/IEEE Standard 802.11: Wireless LAN Standard*, 1999. ISO/IEC 8802-11:1999(E).

[Int84] International Organization for Standardization. "Information Processing Systems – Open Systems Interconnection – Basic Reference Model." ISO 7498-1, Oct 1984.

[Kar90] Karn, Phil. "MACA - A New Channel Access Method for Packet Radio." *ARRL/CRRL Amateur Radio Ninth Computer Networking Conference*, pp. 134–140, 1990.

[KSV00] Ko, Young-Bae, Vinaychandra Shankarkumar, and Nitin H. Vaidya. "Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks." *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, Vol. 1, pp. 13–21. 2000.

[KT75] Kleinrock, Leonard and Fouad A. Tobagi. "Packet Switching in Radio Channels: Part 1-Carrier Sense Multiple-Access Modes and their Throughput-Delay Characteristics." *IEEE Transactions in Communications*, COM-23(12):1400–1416, December 1975.

[OPN01] OPNET Technologies, Inc., 7255 Woodmont Avenue, Suite 250, Bethesda MD, 20814-7904. *OPNET Modeler Modeling Concepts*, 4th edn., 2001.

[PD00] Peterson, Larry L. and Bruce S. Davie. *Computer Networks*. San Francisco: Morgan Kaufmann Publishers, 2000, 2nd edn.

[Rap02] Rapallo, James R., Jr. *A Direct Sequence Code-Division Multiple-Access Local Area Network Model*. Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, March 2002. AFIT/GE/ENG/02M-22.

[SK99] Sobrinho, João L. and A. S. Krishnakumar. "Quality-of-Service in Ad Hoc Carrier Sense Multiple Access Wireless Networks." *IEEE Journal on Selected Areas in Communications*, 17(8):1353–1368, Aug 1999.

[Skl88] Sklar, Bernard. *Digital Commuications: Fundamentals and Applications*. Prentice-Hall, 1988.

[Tan96] Tanenbaum, Andrew S. *Computer Networks*. Upper Saddle River, New Jersey: Prentice Hall PTR, 1996.

[TK75] Tobagi, F. A. and L. Kleinrock. "Packet Switching in Radio Channels: Part II - The Hidden Terminal Problem in Carrier Sense Multiple Access and tbe Busy Tone Solution." *IEEE Transactions in Communications*, COM-23(12):1417–1433, December 1975.

[XS01] Xu, Shugong and Tarek Saadawi. "Does the IEEE 802.11 MAC Protocol Work well in Multihop Wireless Ad Hoc Networks?" *IEEE Communications Magazine*, 39(6):130–137, June 2001.

Vita

2nd Lt. Christopher K. Roberts enlisted in the United States Air Force in July of 1996 and was based at Dyess Air Force Base in Abilene, TX. The following year he enrolled in the United States Air Force Academy where he earned a Bachelor of Science in Computer Science. He graduated and was commissioned in May of 2001.

His first assignment was to the Air Force Institute of Technology at Wright-Patterson Air Force Base in Dayton, OH. There he pursued a Master of Science in Computer Science. Following AFIT, Lt. Roberts will be stationed at Lackland Air Force Base in San Antonio, TX at the 23d Information Operations Squadron.

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
25-03-2003	**Master's Thesis**	Aug 2002 – Mar 2003

4. TITLE AND SUBTITLE ADJUSTING SENSING RANGE TO MAXIMIZE THROUGHPUT ON AD-HOC MULTI-HOP WIRELESS NETWORKS	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Roberts, Christopher, K., 2nd Lieutenant, USAF	**5d. PROJECT NUMBER** 02-055 **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GCS/ENG/03-17
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) NSA/R5 Attn: Mr. William Kroah National Security Agency DSN: (301) 688-0348 Ft. George G. Meade, MD 20755-6000 e-mail: wtk@afterlife.ncsc.mil	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The use of ad-hoc wireless networks is becoming increasingly common within the United States Air Force. Such networks are able to be implemented where traditional wired networks are either impractical or too expensive. As the miniaturization of communication devices continues, it is becoming increasingly common for mobile devices to communicate directly with each other, eliminating the need for central access points. Such a network is referred to as a multi-hop ad-hoc network, or simply a multi-hop network.

Most multi-hop network protocols use some form of carrier sensing to determine if the wireless channel is in use. A large sensing range can reduce packet collisions. However, it can also decrease spatial reuse. Conversely, a smaller sensing range can lead to higher spatial reuse but increase packet collisions.

This study examines a variety of multi-hop network topologies, sizes and traffic loads and determines the sensing range for each that maximizes network throughput. In most instances, a sensing range twice as large as the node's communication range yields maximum or near maximum network throughput. However, results indicate a shorter sensing range can be better if it provides a significant increase in spatial reuse.

15. SUBJECT TERMS

Wireless Communications, Communication Protocols, IEEE 802.11, Clear Channel Assessment

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Rusty O. Baldwin, Major, USAF (ENG)
U	U	U	UU	99	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4612; e-mail: rusty.baldwin@afit.edu